



Perkins Coie LLP
700 13th Street, N.W.
Suite 800
Washington, D.C. 20005-3960

T. +1.202.654.6200
F. +1.202.654.6211
perkinscoie.com

Marc S. Martin
MMartin@perkinscoie.com
D. +1.202.654.6351
F. +1.202.654.9113

February 27, 2025

Brendan Carr
Chairman
Federal Communications Commission
45 L Street NE
Washington, D.C. 20554

Attn: Enforcement Bureau – Telecommunications Consumers Division

Re: Notice of Apparent Liability (NAL/Acct. No.: 202432170009)

Dear Chairman Carr:

As counsel to Telnyx LLC (“Telnyx”), the undersigned submits to your attention its response to the Federal Communications Commission’s (“Commission” or “FCC”) Notice of Apparent Liability for Forfeiture (“Telnyx NAL” or “NAL”), including supporting declarations and exhibits.

We look forward to your response.

Sincerely,

Marc S. Martin
David W. T. Daniels
Michael R. Huston
Brandon R. Thompson
Perkins Coie LLP

Counsel for Telnyx

Enclosure

Executive Summary*

Fraudulent calls are a significant problem for the telecom industry, not to mention a serious annoyance and risk to consumers. That is why voice provider policies and protocols for stopping fraudulent calls are constantly evolving and adapting in response to sophisticated bad actors' tactics and technologies. In the Telnix NAL, the Commission alleges that Telnix violated Section 64.1200(n)(4) of the Commission's Rules (the "Effective Measures" rule). Telnix has consistently used industry best practices to deter often sophisticated bad actors who seek to engage in illegal calls—in many cases going above and beyond what the law requires. But no system of deterring and preventing illegal calls is *perfect*, as the Commission has repeatedly recognized, because industry must always fight to keep up with scammers' evolving tactics and use of advanced technology. Telnix is among the industry's leaders in combating robocalling, and the fact that the bad actor at issue in this case, an entity known as MarioCop, briefly slipped through the cracks does not mean Telnix failed to comply with the Effective Measures rule.

From the tone and tenor of the NAL, the Commission's press release, and the Commission's public statements about how MarioCop contacted Commission personnel and their family members with unlawful calls, it is apparent that this highly targeted and intentional campaign was naturally upsetting to the authors of the NAL.¹ The NAL spends more words describing MarioCop than Telnix in the NAL's "Relevant Parties" section, though MarioCop is not a party to this matter. The NAL's "Factual Background" begins with a discussion of the conduct of MarioCop, not Telnix. The NAL mentions MarioCop 65 times and describes the content of MarioCop's calls on three separate occasions. The Biden administration directed the Enforcement Bureau's investigation almost until the day the NAL was adopted. The outgoing Biden administration ran out the Commission's clock, impairing the ability of Chairman Carr's Commission to closely evaluate the Telnix NAL's regulatory approach to ensure that it is consistent with the policy priorities and directives of President Donald J. Trump. As we will show, it is not.

The NAL downplayed the breadth and focus of the intentionally targeted campaign. In some parts of the NAL, it refers to "eight" Commission employees receiving calls while in others it refers to "over a dozen," but in fact the penetration of the Commission by MarioCop was far more significant. The Commission has not disclosed whether it experienced a security breach that allowed MarioCop to have access to personal cell phone numbers of Commission personnel their family members, but the Commission's decision to punish Telnix for properly and quickly responding to a sophisticated bad actor's brief, single-instance evasion of Telnix's controls is

* We note that Telnix has not requested confidential treatment of anything included in this NAL Response. The Commission released the NAL in a redacted form and delivered an unredacted version to Telnix. For clarity, no content that was redacted by the Commission in the NAL is contained in this NAL Reply.

¹ See, e.g., Brendan Carr (@BrendanCarrFCC), X (Feb. 4, 2025, 9:50 PM), <https://archive.is/H9O9v>; The FCC (@FCC), X (Feb. 4, 2025, 4:29 PM) (referring the Commission's action as being in response to MarioCop's calls), <https://archive.is/cNejt>; Federal Commc'ns Comm'n, Press Release, *First Commission-Level Vote Under Chairman Carr Proposes A Nearly \$4.5 Million Fine Stemming From Apparently Illegal Robocall Scheme* (Feb. 4, 2025) (describing the violation as stemming from MarioCop's conduct).

misguided, inconsistent with the governing statutes and regulations, without precedent or fair notice, and unconstitutional. The NAL must be rescinded for the following reasons:

1. Telnix did not violate the Effective Measures rule.

Telnix met or exceeded the requirements of the Commission’s Effective Measures rule. The rule clearly requires only that a provider take “affirmative, effective measures” to prevent “illegal calls,” including “knowing its customers” as well as “due diligence,” to avoid misuse of the network.² But the Telnix NAL rewrites the rule to impose strict liability for the know your customer requirement without regard to compliance with the Effective Measures standard that obviously modifies any such requirement as is plain from the word “including.” As enforced, the Telnix NAL does not provide “fair warning of the conduct [the regulation] prohibits or requires” or “a reasonably clear standard of culpability”³ as required under President Trump’s executive orders.⁴ The NAL cannot be reconciled with the Commission’s repeated statements that it did not expect “perfection” or that providers’ Effective Measures would need to be “completely effective.”⁵ Enforcement of the rule to now require perfection is the sort of “unfair surprise” proscribed by President Trump’s executive orders.

The NAL’s finding of an alleged Effective Measures violation also conflicts with the Commission’s stated intention to provide industry with flexibility to keep pace with changes in technology and tactics utilized by the bad actors. The Commission has always recognized that a provider complies with the Effective Measures rule by implementing reasonable *ex ante* controls and should not be punished because a single, sophisticated bad actor managed to briefly elude those controls. The Commission’s prior statements to that effect are the best interpretation of the governing statutes.

Telnix has a longstanding track record as a responsible actor in the robocall mitigation ecosystem and proudly employs Effective Measures that demonstrably prevent bad actors from accessing Telnix’s network. To illustrate that point, (i) Telnix is a member of approximately 20 different industry organizations and working groups, many specifically targeted at mitigation of illegal traffic, (ii) Telnix blocks approximately half of all attempted new customer signups due to its stringent fraud mitigation measures, and (iii) only about 0.2% of its customers are the subject of a traceback request.

2. The NAL violates at least two of President Trump’s executive orders: Executive Order 13892, which prohibits regulation by enforcement, by surprise, and without transparency; and Executive Order 14219, which calls for rescinding unconstitutional and improperly interpreted *Chevron*-era regulations.

² 47 C.F.R. § 64.1200(n)(4).

³ See, e.g., *Diamond Roofing Co. v. Occupational Safety & Health Rev. Comm’n*, 528 F.2d 645, 649 (5th Cir. 1976); *Kropp Forge Co. v. Sec’y of Lab.*, 657 F.2d 119, 122 (7th Cir. 1981) (cited in Executive Order 13892).

⁴ See, e.g., *infra*, ¶¶ 20-22.

⁵ *In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, 35 F.C.C. Rcd. 15221, 15233 (Dec. 29, 2020).

The Commission's investigation in this proceeding was carried out almost entirely under the direction of former Chairwoman Jessica Rosenworcel during the Biden administration. During that time, Telnix fully cooperated with the Commission's investigation, with the understanding that the shared goal was to identify the bad actors responsible for the illegal calls that were behind the MarioCop accounts. Facing the imminent expiration of the one-year statute of limitations on February 6, 2025, Enforcement Bureau staff requested a three-month tolling agreement from Telnix. Telnix denied that request, and the Commission hastily rushed to adopt the NAL just two days later.

Meanwhile, as one of his first acts after being sworn in for his second term, President Trump reinstated Executive Order 13892 – *Promoting the Rule of Law Through Transparency and Fairness in Civil Administrative Enforcement and Adjudication* (“E.O. 13892”). The Telnix NAL, presumably largely written before President Trump's inauguration, disregards all three components of E.O. 13892: the prohibition of regulation by enforcement, unfair surprise, and lack of transparency in federal agency enforcement proceedings. Shortly thereafter, President Trump signed two additional executive orders. The first, Executive Order 14215 – *Ensuring Accountability for All Agencies* (“E.O. 14215”), further clarified what was already true: E.O. 13892 applies to independent agencies like the Commission. The second, Executive Order 14219 – *Ensuring Lawful Governance and Implementing the President's “Department of Government Efficiency” Deregulatory Initiative* (“E.O. 14219”), calls on the heads of all agencies, independent or otherwise, to identify for rescission all potentially unconstitutional regulations, those that “are based on anything other than the best reading of the [statute],” and those that “harm the national interest by significantly and unjustifiably impeding technological innovation.”

In its haste to issue the NAL before the expiration of the statute of limitations, the Commission apparently lacked sufficient time to review how the NAL heavily relies on discredited Obama- and Biden-era legal theories as the basis for alleging liability, and how it violates President Trump's executive orders. The NAL contorts an intentionally flexible rule and transforms it into a cudgel for punishing a voice provider for the unlawful calls of a single unrelated bad actor. Among other things, the NAL cites as its lone “precedent” a consent decree that was not published until six months after the alleged violation by Telnix. President Trump's E.O. 13892 specifically requires that “agencies shall afford regulated parties the safeguards described in this order, *above and beyond* those that the courts have interpreted the Due Process Clause of the Fifth Amendment to the Constitution to impose.” The result is a NAL that violates Telnix's fundamental due process rights.

3. The Due Process Clause and the Commission's governing statutes require recusal of any member with a personal connection to the case; therefore, the Commission must either re-vote to cure any conflict of interest or cancel the NAL.

Commission employees (current and past) and their families were the primary and intentional targets of the calls placed by MarioCop. The persons reached include the current Chairman of the Commission, the Chairman of the Commission during President Trump's first term, one current commissioner, numerous chiefs of staff, legal and policy advisors in the offices of all of the current commissioners and the last two Commission chairs, members of the front offices of the Enforcement Bureau, the Office of General Counsel, the Wireline Competition Bureau, the Office of the Managing Director, and staff attorneys of such bureaus and divisions,

family members of Commission personnel, and other government officials and industry participants in the telecom policy ecosystem.

Personal cell phone numbers of Commission personnel are not made publicly available by the agency, and the identities and personal cell phone numbers of their family members are not, either. Adding to the mystery of how or why it occurred, the NAL downplays the magnitude of the Commission's apparent significant security breach that enabled these unlawful calls by inaccurately listing a small number of personnel who received calls from MarioCop. The NAL did not (i) publicly acknowledge its apparent security breach, disclose whether it conducted an investigation into how these private cell phone numbers and family member identities were leaked, (ii) describe what steps it took to ensure the impartiality of an in-house adjudicatory proceeding, and (iii) ensure that the Commission carried out this investigation in compliance with its duty under the Due Process Clause and related statutes to ensure the impartiality of the Commission's actions. For these reasons, Telnyx requests that the Commission, including its inspector general, investigate whether the Commission's impartiality was influenced by being personally targeted by MarioCop. If so, this appears to be the first case where voting members of the Commission (let alone the front offices and staff of relevant bureaus) were personally harmed by the conduct that is germane to the NAL. Under these extraordinary circumstances where the Commission's impartiality could reasonably be questioned by the public, the Commission must rescind the votes on the NAL by any member that was personally affected by MarioCop's calls directly or indirectly by calls to family members or advisors. This is a threshold due process issue that the Commission must address before it can properly consider any action against Telnyx.

4. The Commission arbitrarily classifies Telnyx's one-way VoIP offering as a common carrier service for purposes of calculating the proposed fine and to establish legal authority for the Effective Measures rule, both of which rely on discredited Obama- and Biden-era reinterpretations of Title II of the Act.

The Telnyx NAL reads as if President Biden won the 2024 presidential election, the *Chevron* doctrine was not overturned, and the Commission's net neutrality orders were never vacated. The bad actor's calls were made using Telnyx's one-way domestic VoIP service. The NAL asserts that Telnyx should be classified as a Title II common carrier for purposes of calculating the proposed fine because Telnyx was granted an international Section 214 authorization almost 14 years ago. This action is improper because it is well established that a provider should be treated as a Title II common carrier only to the extent the services at issue are Title II services. That is not the case here, so the Title II regulations cannot apply.

Reflecting the discredited Biden era statutory interpretation, the NAL alleges that Telnyx violated a rule that relied on the anti-discrimination provisions of Sections 201 and 202 of the Act as its legal authority. In doing so, the Commission extended the Effective Measure's reach to one-way VoIP providers – who have never before been classified as Title II service providers. That is the obvious meaning of the Commission's statement that, “[a]bsent broad application [of Title II's anti-discrimination provisions], VoIP would remain a safe haven for bad actors.” But the Commission cannot rely on policy arguments to reinterpret the clear statutory distinctions between Title I and Title II. The Supreme Court's overruling of the *Chevron* doctrine in *Loper Bright Enterprises* clarifies that only the best meaning of the statutory text is the law. On that basis, the U.S. Court of Appeals for the Sixth Circuit recently overturned the Commission's 2024

reinstatement of net neutrality based on a similarly expansive reinterpretation of Title II. The Commission’s application of Title II obligations in the NAL rests on substantially the same legal error.

5. This proceeding brings to light the incurable flaws of the Commission’s in-house adjudications for monetary penalties, which the Supreme Court found unconstitutional in *SEC v. Jarkesy*.

Commissioner Simington was correct in his dissent to the NAL that the Commission cannot proceed further with this enforcement action, in which the Commission seeks monetary damages, in light of the U.S. Supreme Court’s 2024 decision in *Jarkesy*. *Jarkesy* makes clear that Telnyx possesses a Seventh Amendment right to a trial by jury because its claims are “legal in nature.” Indeed, the NAL highlights the longstanding due process infirmities identified by well-reasoned critics of the Commission’s in-house enforcement proceedings.

6. The conduct of this proceeding and the issuance of the NAL will chill industry’s willingness to cooperate with the Commission, contrary to the public interest.

Despite Telnyx’s active cooperation in the investigation, the Commission chose to punish Telnyx for a small number of calls that it did not make and which it voluntarily shut down with commendable speed. Telnyx deplors unlawful calls: they cost service providers money, upset subscribers, and harm the reputations of providers, industry, and the Commission. Telnyx is an active participant in Commission-supported anti-robocall working groups and has been an active partner of the Industry Traceback Group (“ITG”) since March 2020, or at least was until the publication of the NAL’s allegations, which caused ITG to “suspend” Telnyx even before issuance of a final order. Telnyx also funds “honeypot” numbers to catch bad actors. The Telnyx NAL sends a chilling and counterproductive message to the telecom industry: no matter how sincere and extensive your cooperation is with the Commission, if you fail to achieve 100% perfection then you may find yourself facing a multimillion-dollar enforcement penalty. The NAL’s unsupported allegations are costing Telnyx significant business, harming its reputation with consumers, and damaging its standing and relationships in the industry.

* * *

The Commission claims that fighting unlawful robocalls is its top consumer-protection priority. In this case, the Commission spent hundreds of hours, substantial resources, and countless taxpayer dollars to punish Telnyx for 1,117 completed calls by a single sophisticated bad actor that relied on non-public information (and an apparent Commission security breach) to intentionally target Commission personnel, before Telnyx swiftly blocked the traffic and shut down the customer within 17 hours. Billions of illegal robocalls flood consumers every month. In line with the President’s directives and the law, the Commission should re-direct its enforcement priorities at the actual bad actors; not companies like Telnyx that have a demonstrated commitment to compliance and a track record of success.

Table of Contents

	<u>Page</u>
Introduction.....	1
I The NAL violates Executive Orders 13892 and 14219.....	1
II The Commission must ensure that its in-house adjudicatory proceeding is impartial and has the appearance of impartiality. It should rescind the NAL.	14
III The Commission wrongly treats Telnyx’s one-way VoIP service as a Title II common carrier service.	19
IV Telnyx Met or Exceeded the Effective Measures Required by the Commission’s Rules.	22
a Telnyx complied with the Effective Measures rule to prevent new and renewing customers from using its network to originate illegal calls.	22
b <i>The Telnyx NAL’s other miscellaneous arguments fail.</i>	31
i Telnyx does not allow “high volume” traffic.	31
ii Telnyx’s Effective Measures were then, and are now, compliant.....	34
iii The NAL’s allusions to other potential measures that “may contribute” to meeting the Effective Measures rule show the Commission has not determined what is required of industry.	37
iv Telnyx’s measures met or exceeded industry standards.	39
V The Commission is violating <i>Jarkesy</i> and other constitutional obligations by bringing an in-house adjudication for monetary penalties without affording Telnyx its constitutional right to a trial by jury.	41
VI Even assuming <i>arguendo</i> there was a violation, there is no factual basis for the allegation that Telnyx engaged in willful or repeated violations of the Commission’s rules.....	45
VII The Monetary Penalty Suggested by the Telnyx NAL Is Arbitrary, Capricious, and an Abuse of Discretion.	48

a	There is no rational connection between the number of illegal calls attempted by MarioCop and an alleged Effective Measures violation.	48
i	<i>The proposed penalty is disproportionate to other volume-based forfeiture orders by the Commission.</i>	48
ii	<i>The proposed penalty wrongly attempts to enforce the TCPA on Telnyx for MarioCop’s illegal calls.</i>	52
b	<i>There is no rational connection between the alleged violation of Section 64.1200(n)(4) and the call blocking rule in Section 64.6305(g)(1).</i>	52
i	<i>The Commission incorrectly analogizes Section 64.1200(n)(4) to Section 64.6305(g)(1).</i>	53
ii	<i>Selecting Section 64.6305(g)(1) constitutes an unfair surprise which contradicts its articulated standards from its proposed rulemaking.</i>	53
VIII	Relief Requested.	54

Exhibits

EXHIBIT A – Declaration of David Casem

EXHIBIT B – Declaration of Tom Walker

EXHIBIT C – Telnyx Letter to the Enforcement Bureau

EXHIBIT D – Consumer Complaints on Telnyx’s Effective Measures Practices

EXHIBIT E – Y Combinator Hacker News Complaint on Telnyx’s Effective Measures Practices

EXHIBIT F – Robocalling Enforcement Action Table

EXHIBIT G – Comparison of Robocall Mitigation Database Filings

Introduction

Telnyx⁶ offers a variety of voice and data services, including communications, IoT, networking and compute services. Like many VoIP providers, Telnyx offers as distinctly separate products a one-way and a two-way interconnected VoIP service. On February 6, 2024, a sophisticated and highly motivated bad actor, MarioCop, created two accounts on Telnyx’s platform and began using Telnyx’s one-way VoIP service (MarioCop could make outbound calls but could not receive calls) to make apparently unlawful domestic calls targeting primarily Commission leadership and staff. Prior to MarioCop making telephone calls using Telnyx’s one-way VoIP service, Telnyx applied its standard customer onboarding measures for Level 1 (i.e., non-high volume) accounts, which included (i) requiring that the customer adopt Telnyx’s Terms of Service and Acceptable Use Policy (ii) obtaining the account holder’s name, physical address, business email address, and IP address, and (iii) an extensive review of the customer by Sift Science, Inc. (“Sift”), Telnyx’s third party fraud mitigation vendor, amongst other measures. Telnyx continued to monitor MarioCop after provisioning and, upon confirming MarioCop’s scheme, blocked all MarioCop traffic within just 17 hours.

I The NAL violates Executive Orders 13892 and 14219.

1. The Telnyx NAL violates due process, the Administrative Procedure Act (APA), and all three core components of President Trump’s E.O. 13892.⁷ Specifically, the Commission’s action (i) constitutes regulation by enforcement, (ii) is based on “unfair surprise,” and (iii) lacks transparency, all of which E.O. 13892 prohibits in federal agency enforcement proceedings.

2. President Trump signed E.O. 13892 on October 9, 2019 before it was rescinded by Biden on January 20, 2021.⁸ On Day 1 of his second term, President Trump promptly rescinded President Biden’s rescission, which restored E.O. 13892’s legal effectiveness. The goal of E.O. 13892 is to rein in the reckless administrative state in its overzealous trampling of Americans’ due process rights.⁹

⁶ Telnyx’s headquarters is located at 600 Congress Avenue, 14th Floor, Austin, TX 78701.

⁷ Promoting the Rule of Law Through Transparency and Fairness in Civil Administrative Enforcement and Adjudication, Exec. Order No. 13892 of Oct. 15, 2019, 84 Fed. Reg. 55239 (Oct. 15, 2019), <https://www.federalregister.gov/documents/2019/10/15/2019-22624/promoting-the-rule-of-law-through-transparency-and-fairness-in-civil-administrative-enforcement-and>.

⁸ President Biden rescinded E.O. 13892 on January 20, 2021, but President Trump reinstated E.O. 13892, in its entirety, prior to the Telnyx NAL on January 20, 2025, through Executive Order 14148 – *Initial Rescissions of Harmful Executive Orders and Actions*. See *Initial Rescissions of Harmful Executive Orders and Actions*, Exec. Order No. 14148 of Jan. 20, 2025, 90 Fed. Reg. 8237 (Jan. 28, 2025). <https://www.federalregister.gov/documents/2025/01/28/2025-01901/initial-rescissions-of-harmful-executive-orders-and-actions>.

⁹ To preempt the argument that E.O. 13892 does not apply to the so-called “independent” agencies. E.O. 13892 states that “‘Agency’ has the meaning given to ‘Executive agency’ in section 105 of title 5, United States Code.” Under 5 U.S.C. § 105, an “‘Executive agency’ means an Executive department, a Government corporation, and an *independent establishment*.” (emphasis added). This interpretation was confirmed in Justice Scalia’s concurrence in *Freytag v. Comm’r of Internal Revenue*, 111 S.Ct. 2631, 2660 (1991) and again by President Trump’s E.O. 14215, which confirmed that all independent agencies answer to the White House in all respects. Even E.O. 14215 essentially

3. E.O. 13892 begins, “The rule of law requires transparency. Regulated parties must know in advance the rules by which the Federal Government will judge their actions.”¹⁰ It adds, “Agencies shall afford regulated parties the safeguards described in this order, above and beyond those that the courts have interpreted the Due Process Clause of the Fifth Amendment to the Constitution to impose.” (Emphasis added). The Commission failed to meet these Presidential directives in the Telnx NAL.

4. The NAL disregards President Trump’s E.O. 13892 and fails to meet the expectations of the White House as to the proper scope and manner of regulatory enforcement. For substantially the same reasons—discussed in more detail below—the NAL violates the APA, the Due Process Clause of the Fifth Amendment, and the Commission’s other governing statutes by (i) creating substantive rules without following the proper procedures, (ii) unlawfully subjecting Telnx to unfair surprise in violation of its due process rights, and (iii) depriving Telnx of fair notice of the conduct that the Commission would fault to assess liability.

5. Telnx brought E.O. 13892 to the Enforcement Bureau staff’s attention on January 30, 2025, before the NAL was adopted. But given the absence of any reference to it in the NAL, it is unclear whether anyone briefed the Commissioners prior to the vote. There is no ambiguity that E.O. 13892 applies to the Commission.¹¹ As E.O. 14215 makes clear: “[independent] regulatory agencies currently exercise substantial executive authority . . . [and] to be truly accountable . . . must be supervised and controlled by the people’s elected President.”¹² The accompanying fact sheet to E.O. 14215 explained that the President’s intent is to ensure independent agencies like the Commission remain aligned with and accountable to the White House, as any other federal agency.¹³ The Commission has an opportunity to fulfill President Trump’s mandates by rescinding the NAL.

6. Lastly, E.O. 14219 requires that the Commission identify for rescission regulations that, amongst other criteria, are (i) “unconstitutional regulations and regulations that raise serious constitutional difficulties”; (ii) “regulations that are based on anything other than the best reading of the underlying statutory authority or prohibition”; and (iii) “regulations that harm the national interest by significantly and unjustifiably impeding technological innovation.”¹⁴ Each of the above are implicated by the NAL’s effort to enforce the Effective Measures rule against a one-way VoIP

reconfirmed the same legal conclusion of the Department of Justice’s Office of Legal Counsel memo “Extending Regulatory Review Under Executive Order 12866 to Independent Regulatory Agencies,” issued on October 8, 2019 and available at <https://www.justice.gov/olc/file/1349716/dl?inline>.

¹⁰ E.O. 13892 § 1.

¹¹ See 5 U.S.C. § 105.

¹² White House, *Ensuring Accountability for All Agencies* (Feb. 1, 2025), <https://www.whitehouse.gov/presidential-actions/2025/02/ensuring-accountability-for-all-agencies/>.

¹³ White House, *Fact Sheet: President Donald J. Trump Reins in Independent Agencies to Restore a Government that Answers to the American People* (Feb. 18, 2025), <https://www.whitehouse.gov/fact-sheets/2025/02/fact-sheet-president-donald-j-trump-reins-in-independent-agencies-to-restore-a-government-that-answers-to-the-american-people/>.

¹⁴ E.O. 14219 § 2.

provider in an in-house adjudicatory proceeding seeking monetary fines. Criterion (i) is endorsed by Commissioner Simington himself, who stated in his dissent that he voted against the NAL because it is unconstitutional under *Jarkesy*.¹⁵ Criterion (ii) is triggered by the Commission’s Biden-era expansive reinterpretation of Title II as legal authority to regulate a non-Title II service in contravention of the best reading of the statute, departing from the courts’ instructions in *Loper Bright Enterprises* and *Ohio Telecom Association v. FCC*.¹⁶ And criterion (iii) is triggered by the NAL’s reinterpretation of the Effective Measures rule to impose a new strict liability standard, which will necessarily impede technological innovation in industry’s adoption of new fraud mitigation systems, particularly with regard to the use of artificial intelligence (AI) and machine learning. And E.O. 14219 speaks directly to agency enforcement actions, requiring that “agencies [] preserve their limited enforcement resources by generally de-prioritizing actions to enforce regulations that are based on anything other than the best reading of a statute,” and “[a]gency heads shall determine whether ongoing enforcement of any regulations identified in their regulatory review is compliant with law and Administration policy.”¹⁷ The NAL was announced with fanfare as the “first” enforcement action of the new Commission, contrary to the E.O.’s direction to “de-prioritize” enforcement actions squarely at odds with the President’s priorities.

7. As discussed further below, the Effective Measures Rule requires only *reasonable* mitigation against fraudulent calls.¹⁸ That requirement has never been understood to require perfection—indeed, the Commission’s own record expressly clarifies that perfection is *not* required. The reason is obvious: the Commission had admitted that sometimes a bad actor will evade even “effective” measures, which is why imposing liability for calls placed—without more—is not a sufficient ground for liability. Bad actors are also constantly adapting to new technology to evade controls, causing industry to respond with new and evolving counter-measures, as anticipated by the Commission in the very rules it now claims Telnix violated. Here, for the first time and without fair notice, the Commission transforms that simple Effective Measures requirement into a strict liability standard for Know Your Customer (KYC). The upshot of the Commission’s legal interpretation underlying the NAL is that, if a single bad actor evades detection, then a provider’s measures must be ineffective. But the Commission has never promulgated rules to that effect. Instead, it issued an NAL that can be understood only as reinterpreting the Effective Measures rule, effectively “regulation by enforcement.” In doing so, the Commission failed to afford Telnix with fair notice, subjected Telnix to unfair surprise, and engaged in a targeted campaign devoid of transparency. In this way, the Commission violated all three tenets of E.O. 13892.

Regulation by Enforcement.

“I will also be focused on ensuring that the FCC does not undertake ‘rulemaking through enforcement’ by creating new, substantive obligations that go beyond the standards set forth in our existing rules. We need to be careful that we do not

¹⁵ Telnix NAL, ¶ 15 (Comm’r Simington Dissent).

¹⁶ See Section III, *infra*.

¹⁷ E.O. 14219 § 3 (emphasis added).

¹⁸ See Section IV, *infra*.

undermine reasonable reliance on prior FCC decisions and spring enforcement on parties seeking to comply in good faith.”¹⁹

– then-Commissioner Brendan Carr in a statement accompanying the Lingo Telecom NAL (May 28, 2024)

8. Other federal agencies have tried regulation by enforcement. It doesn’t work. It harms industry, consumers, and ultimately, the very agencies that deploy it. The non-partisan Financial Services Institute (“FSI”) crafted a list of indicia of regulation by enforcement.²⁰ The Commission’s actions meet many of these indicia:

- Regulatory enforcement action (or an indication of noncompliance) without prior notice of the regulatory obligation, either by law, rule, litigated precedent, or clear explicit guidance. The Commission stated, explicitly, that it does not require “perfection” or expect Effective Measures to be “completely effective.”²¹ The best interpretation of this language is that the Commission recognized that some bad actors would foil providers’ Effective Measures. That the Commission is now imposing strict liability means it is reinterpreting the Effective Measures rule in a new manner without prior notice and comment.
- Prescriptive directives on regulatory obligations established through enforcement of a principles-based rule without prior notice or appropriate guidance. The Effective Measures rule is principles-based. The Commission expressly chose to regulate with a subjective, industry-led approach.²² The Commission touted that its rules allowed “flexibility” to service providers, claimed that it did “not expect perfection,” and expressly stated that it “do[es] not require that voice service providers take specific, defined steps.”²³ Now, however, the Commission claims that Telnix should have followed the “enhanced” obligations agreed to by Lingo Telecom in a consent decree, but appear nowhere in the Commission’s rules. Further, the Commission’s publication of the enhanced obligations agreed to by Lingo Telecom, occurred long after the incident at issue in the Telnix NAL.
- New interpretation(s) of an existing statute or rule not accomplished through rulemaking preceded by notice and comment, which provides stakeholders the opportunity to publicly comment. As stated in greater detail below, the Commission

¹⁹ *In re Lingo Telecom, LLC*, Notice of Apparent Liability for Forfeiture, FCC 24-60, p. 18 (May 28, 2024) (“Lingo Telecom NAL”) (Comm’r Carr Statement), <https://docs.fcc.gov/public/attachments/FCC-24-60A1.pdf>.

²⁰ Peter Chan, et al., *Recommendations to the SEC to Modify its Procedural Framework to Prevent Regulation by Enforcement*, FIN. SERVS. INST. 8 (Jan. 2024), <https://financialservices.org/wp-content/uploads/2024/01/FSI-Recommendations-to-SEC-prevent-Reg-by-Enforcement-2024-01-25-FINAL.pdf>.

²¹ *In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, 35 F.C.C. Rcd. 15221, 15233 (Dec. 29, 2020).

²² See *Lingo Telecom NAL* (Statement of Comm’r Simington); *infra* ¶ 99 (describing how the Commission requested that the CATA Working Group recommend Effective Measures best practices).

²³ *In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, 35 F.C.C. Rcd. 15221, 15232 (Dec. 29, 2020).

subverted due process and is creating new requirements *ex nihilo* without any industry comment.

9. Regulation by enforcement is antithetical to the requirements of the APA and the Due Process Clause. The Democrat administrations and agencies that have embraced the practice (specifically, financial regulators during the Obama and Biden Administrations) have been chastised with scathing criticism from within the agencies themselves, by regulated industry, and by learned commentators. It is reportedly one of the reasons that President Trump moved quickly after his second inauguration to effectively shut down the Consumer Financial Protection Bureau, which had a reputation for regulation by enforcement, and why the Securities and Exchange Commission (SEC) dropped its enforcement action against Coinbase.²⁴

10. Many SEC commissioners, for example, have strongly opposed regulation by enforcement. In remarks before the Securities Enforcement Forum in 2014, Republican Commissioner Michael Piowar (who later served as Acting Chairman during President Trump’s first administration) stated, “For me, due process starts with fundamental notions of fairness. Persons should be on notice as to what acts, or failures to act, constitute violations of the law and our regulations. Persons should also be on notice as to the potential sanctions and liabilities that may be imposed as a result of those violations.”²⁵ Similarly, in a robust critique of regulation by enforcement in 2022, then-Republican Commissioner and current Acting Chair Mark Uyeda decried the practice, stating:

One significant shortcoming of regulation by enforcement is that it fails to provide a mechanism for the [SEC] to consider the views by market participants, which can result in a myopic approach. In contrast, through the rulemaking process, the public can provide their perspectives on market practices and developments, leading to an informed regulatory response. Regulation through litigation fails to provide these important inputs that result in better crafted rules.

Additionally, regulation by enforcement fails to provide the nuanced and comprehensive guidance that allows market participants to tailor their practices, and instead requires regulated entities to divine how the facts and circumstances of another case apply to their own business model. Market participants should be able to look to the [SEC’s] rules rather than compare how their particular facts and circumstances may differ from those in a specific enforcement case. This principle, while often requiring a longer timeline, and more deliberation, often results in a more transparent and understandable regulatory framework.²⁶

²⁴ Dave Michaels & Vicky Ge Huang, *Coinbase Says SEC Intends to Drop Lawsuit Against Crypto Exchange*, Wall Street J. (Feb. 21, 2025), <https://www.wsj.com/finance/regulation/coinbase-says-sec-intends-to-drop-lawsuit-against-crypto-exchange-4b3b0c36>.

²⁵ Michael S. Piowar, Comm’r, *Remarks to the Securities Enforcement Forum 2014* (Oct. 14, 2014), <https://www.sec.gov/newsroom/speeches-statements/2014-spch101414msp>.

²⁶ Mark T. Uyeda, Comm’r, *Remarks at the “SEC Speaks” Conference 2022* (Sept. 9, 2022), <https://www.sec.gov/newsroom/speeches-statements/uyeda-speech-sec-speaks-090922>.

11. Echoing those statements, David Burton, Senior Fellow in Economic Policy at the Heritage Foundation, chastised agency regulation by enforcement, stating, “Both the SEC and the [U.S. Commodity Futures Trading Commission (CFTC)] have been irresponsible actors in the digital asset area . . . both agencies have chosen regulation by enforcement—and have done it poorly. They neither adequately protect investors nor provide responsible market participants with the regulatory environment that they need to thrive.”²⁷ This is also the position of Jennifer Schulp, Director of Financial Regulation Studies at the CATO Institute, who argues, “Rulemaking achieved through enforcement is suboptimal for many reasons, including simply that it creates worse rules . . . [allowing an agency to] hide the ball, limiting the opportunities of potential respondents to constructively engage with the agency prior to an enforcement action being filed.”²⁸

12. These arguments against regulation by enforcement are now prevailing across the federal government like a breath of fresh air, thanks to President Trump’s E.O. 13892. Indeed, on the very day that the Commission released the Telnix NAL, Caroline Pham, Acting Chair of the CFTC, announced that the agency would “refocus” and “stop regulation by enforcement.”²⁹ President Trump also selected a new SEC Chair that is widely viewed as being favorable to the crypto industry and staunchly against regulation by enforcement.³⁰

13. The NAL’s recitation and apparent endorsement of KYC measures agreed in the Lingo Telecom consent decree is particularly inappropriate. E.O. 13892 states that “[i]f an agency intends to rely on a . . . consent decree . . . it must . . . provide an explanation of its jurisdictional implications.”³¹ The Lingo Telecom Consent Decree was negotiated and resolved between Lingo Telecom and the Commission six months after the factual events giving rise to the Telnix NAL. Because the Lingo Telecom Consent Decree was released after the alleged Telnix violation, the Lingo Telecom Consent Decree (and even the Lingo Telecom NAL that preceded it) obviously cannot serve as fair notice to Telnix. That the NAL even cites the Lingo Telecom Consent Decree highlights the NAL’s lack of notice and its accompanying legal vulnerability under settled judicial precedent. Even disregarding the timing of the Lingo Telecom Consent Decree, consent decrees are not rules of general applicability. As the Ninth Circuit noted in *E.E.O.C. v. Pan Am. World Airways, Inc.*, “It is fundamental to our notions of due process that a consent decree cannot prejudice the rights of a third party who fails to consent to it . . . Likewise, a consent decree cannot

²⁷ *Mandate for Leadership: The Conservative Promise, Project 2025 Presidential Transition Project* at 835, https://static.project2025.org/2025_MandateForLeadership_FULLL.pdf.

²⁸ Jennifer J. Schulp, *Dazed and Confused: Breaking Down the SEC’s Politicized Approach to Digital Assets*, CATO INST. (Sept. 17, 2024), <https://www.cato.org/testimony/dazed-confused-breaking-down-secs-politicized-approach-digital-assets>.

²⁹ Press Release, Caroline D. Pham, Chairman, Commodity Futures Trading Comm’n, Pham Statement on Refocus on Fraud and Helping Victims, Stop Regulation by Enforcement (Feb. 4, 2025), <https://www.cftc.gov/PressRoom/PressReleases/9044-25>.

³⁰ Rafael Nam, *Trump picks crypto backer Paul Atkins as new Securities and Exchange Commission chair*, NPR (Dec. 4, 2024), <https://www.npr.org/2024/12/04/g-s1-36803/trump-crypto-paul-atkins-sec-chair>; Grace Noto, *Trump taps crypto-friendly Mark Uyeda as acting SEC chair*, CFO DIVE (Jan. 21, 2025), <https://www.cfodive.com/news/trump-taps-crypto-friendly-markuyeda-acting-sec-chair/737878/>.

³¹ E.O. 13892 § 5.

prejudice the rights of persons who are strangers to the proceeding, even though they may have actual knowledge of the settlement or the underlying litigation.”³² It speaks to the weakness of the facts and the law relied upon in the Telnix NAL that its sole cited precedent is so obviously improper.

14. In the Lingo Telecom NAL, then-Commissioner Carr and Commissioner Simington both harshly criticized the Rosenworcel-led Commission for engaging in regulation by enforcement, noting it was reinterpreting its rules to hold Lingo Telecom to specific standards without fair notices.

15. Then-Commissioner Carr criticized the Lingo Telecom NAL as regulation by enforcement:

I will also be focused on ensuring that the FCC does not undertake “rulemaking through enforcement” by creating new, substantive obligations that go beyond the standards set forth in our existing rules. We need to be careful that we do not undermine reasonable reliance on prior FCC decisions and spring enforcement on parties seeking to comply in good faith.³³

16. Likewise, Commissioner Simington expressed deep misgivings about the Lingo Telecom NAL’s regulation by enforcement:

Lingo states in its defense that it relied on Life Corp.’s contractual statements about numbers and permissions in what the Enforcement Bureau notes was a one-page form with no diligence backing it up. This might not be the most sympathetic defense, but it isn’t an unreasonable one, because the FCC has never required a higher standard. This is why the FCC has to have recourse to vague statements like “reasonable KYC [know your customer] protocols,” and needs to make a novel finding that a “generic, blanket, check-the-box ‘agreement,’” is insufficient, in order to find liability. All voice providers nationwide are surely taking note of the FCC’s actions today, but it’s not actually clear what their obligations now are. Must they immediately implement KYC and, if so, to what standard? If their current client contracts are inadequate, must they require that all clients sign new ones and, if so, what should the new contracts say? If they fail to do so, should they expect to be fined \$1,000 per call?

These are completely open questions because the FCC has never engaged in a rulemaking on this matter, delegating it instead to an industry group and to industry standards. The problem for our action today is that Lingo probably complied with industry standards. We might deplore the laxity of these standards, but Lingo might well respond that they were in line with actions that had been repeatedly blessed by the FCC. And today, by using an enforcement mechanism to declare new standards (however vague) we are engaged in a back-door rulemaking through enforcement..

³² 897 F.2d 1499, 1506 (9th Cir. 1990); *see also Sierra Club v. N. Dakota*, 868 F.3d 1062, 1067 (9th Cir. 2017).

³³ Lingo Telecom NAL at ¶ 18 (Comm’r Carr Statement) (emphasis added).

. . . the FCC must immediately act to establish clear standards within which the industry can operate.³⁴

17. In the Lingo Telecom Consent Decree, the Commission found that Lingo Telecom applied the incorrect STIR/SHAKEN attestation level to spoofed calls impersonating President Biden, which Lingo Telecom facilitated by effectively neglecting to implement *any* Effective Measures other than a contractual relationship with the party who transmitted the spoofed calls.³⁵ Lingo Telecom’s conduct was fundamentally distinguishable from Telnyx’s conduct in this case. Upon learning from Enforcement Bureau staff that an enforcement action was likely imminent and that the Commission would rely on Lingo Telecom as precedent, Telnyx sent a letter notifying Enforcement Bureau staff of how (i) any such action against Telnyx would violate E.O. 13892, and (ii) the Lingo Telecom enforcement proceeding was not viable precedent. When the Telnyx NAL was published two days later, neither E.O. 13892 nor Telnyx’s letter to the Enforcement Bureau was referenced.³⁶

18. Because Chairman Carr did not release a statement explaining his vote for the Telnyx NAL, it is unclear why he did not stop regulation by enforcement in this proceeding. It appears likely that, given the soon-expiring statute of limitations, there was insufficient time for Chairman Carr’s staff to carefully review the Enforcement Bureau’s draft and see how it was steeped in the Biden era’s regulation-by-enforcement approach and flouted President Trump’s executive orders. To clarify just how novel this action is, the Telnyx NAL appears to be the first time the Enforcement Bureau’s Telecommunications Consumers Division (TCD) has ever cited a consent decree as precedent for an NAL.

19. Both the Lingo Telecom and the Telnyx NALs involve enforcement of the Effective Measures rule, but with Telnyx, the target is a longstanding compliant provider who implemented robust measures and robocall mitigation procedures and who has a long history of good faith cooperation with the Commission and in working with other providers in industry to reduce unlawful calling. How do Lingo Telecom and Telnyx’s facts compare? Lingo Telecom apparently did not correctly implement STIR/SHAKEN. Telnyx has fully implemented STIR/SHAKEN. Lingo Telecom reportedly had functionally no Effective Measures. Telnyx utilized industry best practices for Effective Measures. Lingo Telecom did not participate in any industry bodies. Telnyx is a proud member of the Call Authentication Trust Anchor (CATA) Working Group and the Numbering Administration Oversight Working Group (NAOWG) and works regularly with the Commission to develop industry standards. Telnyx blocked the MarioCop calls within 17 hours, notified the Commission within 24 hours, and met repeatedly and cooperatively with the Commission during the investigation. Lingo Telecom reportedly allowed more than four times the number of completed calls as Telnyx; however, the Telnyx proposed fine is nearly 4.5 times the amount agreed in the Lingo Telecom Consent Decree (\$1 million vs. nearly \$4.5 million). The only rational explanation for the disparate treatment is the content of the calls (block quoted

³⁴ Lingo Telecom NAL at ¶¶ 20 (Comm’r Simington Statement) (emphasis added).

³⁵ Lingo Telecom NAL at ¶¶ 15, 20.

³⁶ See Letter from Marc Martin, Counsel, Telnyx, to Daniel Stepanicich, Deputy Division Chief, Telecommunications Consumers Division, Enforcement Bureau (Jan. 30, 2025) (“Exhibit C”).

upfront in the Telnix NAL) and the identity of the harmed parties (the Commission senior leadership and family members).

Unfair Surprise.

20. Under E.O. 13892, the Commission is prohibited from imposing “unfair surprise” on regulated parties:

When an agency takes an administrative enforcement action, engages in adjudication, or otherwise makes a determination that has legal consequences for a person, it may apply only standards of conduct that have been publicly stated in a manner that would not cause unfair surprise. An agency must avoid unfair surprise not only when it imposes penalties but also whenever it adjudges past conduct to have violated the law.³⁷

21. E.O. 13892 defines “unfair surprise” as “a lack of reasonable certainty or fair warning of what a legal standard administered by an agency requires. E.O. 13892 states that the meaning of this term should be guided by certain listed examples of lack of fair notice discussed by the Supreme Court in *Christopher v. SmithKline Beecham Corp.*”³⁸ That is, E.O. 13892 incorporates *SmithKline Beecham*, among other cases, within the definition of “unfair surprise” as the touchstone for what E.O. 13892 prohibits.

22. In *SmithKline Beecham*, the Court described several examples of lack of fair notice and unfair surprise. In one such example, *Kropp Forge Co. v. Secretary of Labor*, the Seventh Circuit found that the plain language of the regulation (“a continuing *effective* hearing conservation program shall be administered”) did not articulate any elements that such a program must contain, and the agency did not provide evidence of a “common understanding” of what the regulation required.³⁹ The Court further determined that penal application of the regulation’s requirement to merely provide “a continuing effective . . . program” (i) “miss[ed] the mark considerably,” (ii) made the regulation unenforceable, and (iii) provided no warning that the company’s program violated the regulation.⁴⁰ Likewise, in *Dravo Corp. v. Occupational Safety & Health Review Commission*, the Third Circuit held that regulations imposing penal sanctions must provide “adequate notice in the regulations of the exact contours of [a regulatee’s] responsibility.”⁴¹ Here, the Effective Measures rule does not provide any contours of a provider’s responsibility, other than that the program be “effective.”

23. The Supreme Court has already admonished the Commission for attempting to penalize regulated parties without fair notice. In *F.C.C. v. Fox Television Stations, Inc.*, the Court determined that the Commission did not provide fair notice that brief nudity would violate its

³⁷ E.O. 13892 § 3.

³⁸ 567 U.S. 142, 156 & n.15 (2012).

³⁹ 657 F.2d 119, 122-24 (7th Cir. 1981).

⁴⁰ *Id.* at 122.

⁴¹ 613 F.2d 1227, 1234 (3d Cir. 1980).

indecent standards when the Commission’s prior statements would have led to the opposite conclusion.⁴² According to the Court, “[a] conviction or punishment fails to comply with due process if the statute or regulation under which it is obtained ‘fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement.’” As this Court has explained, a regulation [lacks fair notice] not because it may at times be difficult to prove an incriminating fact but rather because it is unclear as to what fact must be proved.⁴³ The Court went on to state that lack of fair notice implicates “at least two connected but discrete due process concerns: first, that regulated parties should know what is required of them so they may act accordingly; second, precision and guidance are necessary so that those enforcing the law do not act in an arbitrary or discriminatory way.”⁴⁴ The Commission should not make the same mistakes here, relying on a regulation that imposes a requirement only that a program be “effective,” and pretending that is sufficient to guide industry conduct.

Discriminatory Enforcement and Unclear Facts.

24. Discriminatory enforcement. As mandated by *Diamond Roofing Co. v. Occupational Safety & Health Review Commission* (another case referenced in E.O. 13892), regulations “must provide a reasonably clear standard of culpability to circumscribe the discretion of the enforcing authority and its agents.”⁴⁵ Yet, despite Telnix’s adherence to the Effective Measures rule, the Commission misrepresented this action as a “crack down” on an “apparently illegal robocall scheme”⁴⁶ and targeted the specific conduct at issue here apparently because it was the primary victim of the MarioCop calls. Targeted, meritless enforcement actions such as this have real-world consequences. Telnix’s CEO has received death threats, and Telnix has lost customers, was suspended from its role as a supporting partner of the ITG, and was placed on probation by the i3Forum—all as a consequence of the allegations in the Telnix NAL. That reputational damage cannot be undone. Years and years of building a trusted brand, establishing relationships, working on anti-robocall efforts with other stakeholders, garnering good will—all gone. This is not how a notice of allegations should work.

25. Unclear as to what facts must be proved. The Commission’s action ignores that, just five months before the NAL, it released a draft order (“Draft Eighth Report and Order”) that would, if adopted, provide more specific rules defining and enforcing a violation for failing to maintain an Effective Measures program (“Draft Requirements”). The Draft Requirements would (i) set the base forfeiture amount at \$11,000 per violation that would “appl[y] on a per-customer, rather than per-call, basis,”⁴⁷ (ii) cap continuous violations at the period in which “the customer

⁴² See generally 567 U.S. 239 (2012).

⁴³ 567 U.S. 239, 253 (citation omitted) (emphasis added).

⁴⁴ *Id.* (citation omitted).

⁴⁵ 528 F.2d 645, 649 (5th Cir. 1976).

⁴⁶ Brendan Carr (@BrendanCarrFCC), X (Feb. 4, 2025, 9:50 PM), <https://archive.is/H9O9v>.

⁴⁷ *In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, Eighth Report and Order, FCC-CIRC2409-02, para. 31 (circulated Sep. 5, 2024) (hereinafter “Draft Eighth Report and Order”), <https://docs.fcc.gov/public/attachments/DOC-405219A1.pdf>.

remains a customer,”⁴⁸ and (iii) set a forfeiture maximum consistent with the maximum amount permitted for non-common carriers.⁴⁹ The Draft Requirements are the only portion of the Draft Eighth Report and Order that relates to the Effective Measures rule.⁵⁰ The docket in ECFS has numerous comments since the Draft Eighth Report and Order’s release, showing widespread industry engagement. But the Telnix NAL fails to mention the Draft Eighth Report and Order or acknowledge industry’s confusion about the Commission’s shifting requirements. In addition, the Telnix NAL proposes to enforce a penalty calculation that is far in excess of the Draft Requirements.

26. The Cloud Communications Alliance (CCA), which includes over 150 companies in the cloud communications sector, agrees that the Effective Measures rule does not require that a provider infallibly know every customer. In response to the Commission’s *Seventh Report and Order and Eighth Notice of Proposed Rulemaking* on the subject,⁵¹ CCA stated:

The Alliance is concerned that the assessment of a forfeiture on these articulated grounds may not afford providers sufficient notice of the prohibited conduct that may warrant financial penalties. The Commission has not defined with any specificity what measures it expects industry to undertake and specifically declined to provide further specificity in the accompanying Seventh Report and Order. Instead, the Commission has deliberately allowed providers flexibility in adopting appropriate mitigation measures. . . . Adopting and complying with a reasonable mitigation plan should constitute a defense to liability.⁵²

27. Shortly after the release of the Draft Eighth Report and Order, the Voice on the Net Coalition (VON) submitted a similar comment to the Commission, stating:

Even providers acting in good faith could be subject to these high forfeitures because it is unclear what standards the Commission will apply to determine whether a provider took ‘affirmative, effective measures’ to prevent its customers from originating illegal calls, including know your customer requirements and exercising due diligence. The rule simply states the obligation.⁵³

⁴⁸ *Id.*

⁴⁹ *Id.*

⁵⁰ Former Chairman Ajit Pai introduced the practice of releasing draft orders as a major reform one month into his term as Chairman during President Trump’s first term. Daniel Lyons, “Chairman Pai’s Legacy of Transparency | American Enterprise Institute - AEI”, (January 21, 2021).

⁵¹ *See generally In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, Seventh Report and Order in CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking in CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59, FCC 23-37, <https://docs.fcc.gov/public/attachments/FCC-23-37A1.pdf>.

⁵² Letter from Michael H. Pryor, Counsel for the Cloud Communications Alliance, to the Federal Communications Commission, at 15-16 (Aug. 9, 2023).

⁵³ Letter from Glenn S. Richards, Couns. to Voice on the Net Coal., to Marlene H. Dortch, Sec’y FCC, at 2 (Sep. 19, 2024) (“VON Comments”), https://www.von.org/filings/year/22_2024/2024_09_19_VON_robocall_ex_parte_FINAL.pdf.

28. VON also took exception to the Commission’s reliance on the Lingo Telecom Consent Decree, warning that the obligations placed on Lingo Telecom “should not be foisted on other voice service providers in violation of the APA.”⁵⁴ VON ultimately concluded that “[s]ervice providers are thus left with no indication of how to comply with the Commission’s rules unless they strive for [] ‘perfection,’ which the Commission claims not to require.”⁵⁵

29. INCOMPAS, the internet and competitive networks association, echoed CCA and VON:

INCOMPAS seeks to align itself with the comments of the VON Coalition which similarly urges the Commission to modify this proposal in order to ensure that “[a]ny fines imposed on originating service providers should be grounded in evidence demonstrating that the provider was aware that its network was involved in facilitating illegal calls and failed to take remedial measures.” INCOMPAS is concerned that such a proposal, without modification, could dramatically expand current legal standards and inadvertently create exposure for compliant voice service providers beyond just those that intentionally facilitate illegal robocalling or intentionally neglect the Commission’s rules.⁵⁶

30. CCA, VON, and INCOMPAS are right. As made clear by the confusing bases for legal liability asserted in the NAL, it is apparent the Commission is attempting to punish conduct that no reasonable industry participant would deem to be unlawful and for which there is no “common understanding” concerning what constitutes a violation of the rules. The rules on which it relies fail to give effective notice of what conduct is required, and what facts the Commission must prove to establish an allegation (and what facts Telnyx can offer to defend itself). That is fundamentally unfair and antithetical to the Commission’s constitutional and statutory obligations to provide fair notice, as confirmed by President Trump’s recent orders.

31. Two days after it released the Telnyx NAL, the Commission issued an updated draft of the Draft Eighth Report and Order (the “Updated Draft Eighth Report and Order”), which the Commission is set to vote on at the Open Commission Meeting on February 27.⁵⁷ The Updated Draft Eighth Report and Order removed the Draft Requirements without comment or explanation. As a result, the Commission is choosing to remove the Draft Requirements as a rule of general application as it simultaneously pursues more stringent requirements in the enforcement proceeding against Telnyx. Thus, the Commission is not even trying to hide its regulation by

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ Letter from Christopher L. Shipley, Executive Director of Public Policy, INCOMPAS, to the Federal Communications Commission, at 6 (Sep. 8, 2023) (referencing an August 9, 2023 letter from VON to the Commission that made the same arguments quoted herein), [INCOMPAS Reply Comments - Dockets No. 17-59, 17-97 \(9.8.23\).pdf](#).

⁵⁷ As of the date of submission of this Telnyx NAL response, the Commission had not yet released the final Eighth Report and Order.

enforcement and unfair surprise against Telnyx even as it declines to adopt a more stringent rule of general application in a pending rulemaking proceeding.

Further APA and Due Process Considerations.

32. As noted above, when an agency wishes to change a substantive regulation, it must go through the notice-and-comment procedure to ensure regulated entities obtain fair notice.⁵⁸ The Commission’s own regulations acknowledge as much, requiring that “prior notice of proposed rulemaking [] be given” and “[a] reasonable time [] be provided for submission of comments in support of or in opposition to proposed rules.”⁵⁹

33. Both the APA and the Due Process Clause forbid abrupt changes through ad-hoc adjudications.⁶⁰ And the Commission’s position is particularly egregious where it fails to even acknowledge that it is changing its view of the underlying regulations—in violation of the fundamental principle of administrative law that the Commission is “obligated to supply a reasoned analysis for the change.”⁶¹

34. Lastly, in December of 2024, the Commission released an Order identifying more than 2,400 voice service providers with deficient robocall mitigation plans (the “RMD Cure Order”)—approximately 30% of voice service providers listed in the Commission’s Robocall Mitigation Database. The Commission noted that these providers’ plans were “deficient because they lack required information” including, inter alia, “a description of the effective measures it is taking to prevent new and renewing customers from originating illegal robocalls,” which is the section of the Rules at issue here.⁶² The Commission notified these providers of the alleged deficiencies by letter on March 29, 2024, nearly two months after the MarioCop calls, and again via the RMD Cure Order, when the Commission’s enforcement action against Telnyx was well-underway. But Telnyx was not identified as possessing a deficient robocall mitigation program. The Commission was well-aware of Telnyx’s Effective Measures, both through Telnyx’s subpoena responses and its RMD filing. By not citing any deficiencies, the Commission has tacitly approved Telnyx’s robocall mitigation plan and its Effective Measures, which were those used when onboarding MarioCop. To suggest now that those measures were not effective is an unfair surprise to the settled expectations of the voice provider industry.

⁵⁸ See *Long Island Care at Home, Ltd. v. Coke*, 551 U.S. 158, 170–71, (2007); *Nat’l Lab. Rels. Bd. v. Bell Aerospace Co.*, 416 U.S. 267, 295 (1974).

⁵⁹ See 47 C.F.R. §§ 1.412, 1.415 (2025).

⁶⁰ See, e.g., *Calumet Shreveport Refin., LLC v. EPA*, 86 F.4th 1121, 1134-1137 (5th Cir. 2023) (finding that an agency’s adjudications based on applying new and different standards of conduct were illegally retroactive), cert. granted on other grounds, 2024 WL 4529794 (Oct. 21, 2024).

⁶¹ *Motor Vehicle Mfrs. Ass’n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 42 (1983).

⁶² See *In re 2,411 Robocall Mitigation Database Filers*, Order, DA 24-1235 ¶¶ 3, 6 (FCC Dec. 10, 2024) <https://docs.fcc.gov/public/attachments/DA-24-1235A1.pdf>.

Lack of Transparency.

35. E.O. 13892 requires that agencies “act transparently and fairly with respect to all affected parties, as outlined in this order, when engaged in civil administrative enforcement or adjudication.” It further encourages agencies to “foster greater private-sector cooperation in enforcement, promote information sharing with the private sector, and establish predictable outcomes for private conduct.” The Commission’s adoption of a novel interpretation of the Effective Measures rule in the Telnix NAL, fails to comply with E.O. 13892’s requirement of transparency.

36. There is nothing predictable or transparent about the Commission’s approach to enforcement in this proceeding. Moreover, it did nothing to foster cooperation. Mere days before the statute of limitations was set to expire, TCD staff contacted Telnix and asked that Telnix enter into a tolling agreement. TCD staff refused to state the purpose of the tolling agreement, what rules the Commission believed that Telnix may have violated, or the legal basis for an enforcement action. After receiving a draft tolling agreement and raising these initial questions, Telnix (at the Commission’s request) met with TCD staff who, when asked if an action was pending, refused to answer. Telnix then asked whether there was any benefit to entering into the tolling agreement, and again, TCD staff refused to answer. This was after Telnix spent months assisting the Commission with its investigation. Lacking a basis to offer informed consent to the tolling agreement request, Telnix declined. The Commission then rushed to adopt an NAL just days before the expiration of the statute of limitations that was replete with errors and inconsistencies.

37. In short, the outgoing Biden administration ran out the Commission’s clock and left Chairman Carr’s new leadership team insufficient time to carefully review and confirm whether the draft NAL was aligned with President Trump’s policies and directives. It is not. The Commission should rescind the NAL so that it may re-evaluate the facts and circumstances here, especially Telnix’s demonstrated record of cooperation and compliance. But more questions remain as a result of MarioCop’s direct harms to Commission personnel and family members, as discussed below.

II The Commission must ensure that its in-house adjudicatory proceeding is impartial and has the appearance of impartiality. It should rescind the NAL.

38. After Telnix received a copy of the NAL, it immediately reviewed the MarioCop call detail records again. As explained in the accompanying Declaration of Tom Walker,⁶³ a respected telecommunications fraud manager, analyst, and investigator with over 20 years of experience, that inquiry proceeded by using publicly-available resources to ascertain the identities of the call recipients in the MarioCop call detail records. In deference to the NAL, Telnix began its analysis under the working assumption that the Commission had accurately described the nature of MarioCop’s calls—that this calling campaign unintentionally reached a small number of Commission staff.”⁶⁴

⁶³ See generally Declaration of Tom Walker (“Exhibit B”).

⁶⁴ Telnix NAL at ¶¶ 5-6, 25.

39. It quickly became apparent that the Commission's reference to "eight" or "over a dozen" in-house victims was a significant understatement. In fact, the Commission was the *intentional* target of an extensive campaign. In total, Walker determined that MarioCop placed calls to at least 365 unique phone numbers associated with Commission offices, staff, and former staff.⁶⁵ In particular, Telnix identified the following recipients of MarioCop's calls:⁶⁶

1. Chairman Brendan Carr,
2. Commissioner Nathan Simington,
3. Former Chairman Ajit Pai,
4. Chiefs of staff, legal and policy advisors in the offices of Chairman Carr, former Chairwoman Rosenworcel and former Chairman Pai, and Commissioners Simington, Gomez and Starks,
5. Numerous senior leadership in the front offices and divisions of the Enforcement Bureau, Office of General Counsel, Wireline Competition Bureau, Office of the Managing Director, among others,
6. Staff attorneys and other personnel throughout the agency, including field offices,
7. Family members of many of the above, and
8. House Majority leadership, NTIA personnel, Department of Justice personnel and other telecom-related policy makers and participants.⁶⁷

40. This same information was discernible from the call data Telnix voluntarily provided to the Commission (and as the recipients, the Commission would be aware of these calls in any event). The Commission stated that it does not make publicly available the personal cell phone numbers of its personnel or those of its family members.⁶⁸ But despite the unusual reliance on non-public information, the NAL minimizes the magnitude of the apparent security breach by describing the number of calls to the Commission as "eight" and "over a dozen," which is as accurate as saying eight (or over a dozen) viewers watched the Super Bowl.⁶⁹ The NAL also downplays the authority of the recipients as "staff." The term "staff" is rarely used to describe two

⁶⁵ Exhibit B, ¶ 8.

⁶⁶ *Id.*, ¶ 7. For clarity, the Commission made the call destination information germane in the unredacted version of the NAL when it stated that MarioCop called the Commission and its personnel. When the Commission did assert confidentiality in the Telnix NAL, it did so without providing any rationale or consistency. For example, the Commission asserted confidentiality for some names but not others, some titles but not others, and for the Commission itself on some occasions but not others. *See* Telnix NAL, n.17.

⁶⁷ *See* Exhibit B, ¶ 8.

⁶⁸ *See* Telnix NAL at ¶ 5.

⁶⁹ *See* Telnix NAL at ¶¶ 5-6, 25.

Senate-confirmed Chairs and one Commissioner, among other senior personnel of considerable authority. By not disclosing this critical information, the NAL avoids raising obvious red flags, such as how did these personal cell phone numbers become available to the bad actor? We do not know, and the Commission has not publicly stated whether it has taken any steps to investigate this apparent security breach. The Commission requires the public to comply with a duty of candor in communications with the agency; the agency should adopt a similar commitment for the public's benefit.

41. Indeed, as an example how readers interpreted the NAL's description of the calls, a reputable tech reporter from Ars Technica inferred that a small number of potentially low ranking FCC staff with positions unrelated to the NAL were "obviously" unintentional collateral damage in a larger robocalling scheme.⁷⁰ Quite the contrary—it is obvious that the Commission itself was the target. Ars Technica was not alone in its mistaken inference. Shortly after the NAL was published, TCPAWorld, Breitbart, Gizmodo, and Lowyat, among others, came away believing that MarioCop must have inadvertently called a few Commission staffers:

- "This story is just baffling to me. Imagine being so dumb, so dumb that you create a robocall scheme where you try to defraud staff at the primary federal regulator that oversees robocalls."⁷¹
- "[R]obocallers posing as employees of the FCC inadvertently targeted real FCC staff members and their families."⁷²
- "If for whatever reason you decide that you want to start up a scam call operation, one thing you should try to avoid, if possible, is calling the very people you are posing as. Unfortunately, no one warned the two imposters of this when they decided to pose as members of the FCC 'Fraud Prevention Team' and they ended up calling FCC staff members."⁷³
- "Robocallers posing as the US Federal Communications Commission (FCC) recently had an 'oh crap' moment when the group accidentally tried to scam employees of the very body they were pretending to be."⁷⁴

⁷⁰ Jon Brodtkin, *Robocallers posing as FCC staff blocked after robocalling real FCC staff*, Ars Technica (Feb. 5, 2025 7:05 PM), <https://archive.is/wALR9#selection-1139.9-1139.81> ("Obviously, robocallers posing as FCC employees probably wouldn't intentionally place scam calls to real FCC employees.").

⁷¹ Eric Troutman, *DUMBEST SCHEME EVER?: FCC Proposes \$4.5MM Penalty on Carrier Telnix LLC After Bad Guys Pose as the FCC...*, TCPAWorld (Feb. 17, 2025), <https://archive.is/Y7F3U#selection-353.0-353.103>.

⁷² Lucas Nolan, *Busted: Robocall Scammers Impersonating the FCC Shut Down After Targeting *Real* FCC Staffers*, Breitbart (Feb. 8, 2025), <https://archive.is/32f21#selection-985.6-985.113>.

⁷³ AJ Dellinger, *Scammers Posing as FCC Fraud Team Call the FCC, Get Fined*, Gizmodo (Feb. 6, 2025), <https://archive.is/Kv4ml#selection-367.9-367.66>.

⁷⁴ John Law, *Robocallers Impersonating The US FCC Calls Actual Government Body By Mistake*, Lowyat (Feb. 7, 2025), <https://archive.is/YF7D4>.

42. As the Supreme Court noted in *Withrow v. Larkin*, “[T]he combination of investigative and adjudicative functions [within an agency] does not, without more, constitute a due process violation,” but, importantly, “special facts and circumstances” may create a “risk of unfairness [that is] intolerably high.”⁷⁵ The Court also implied that courts should examine whether an agency’s conduct evinced a “risk of bias or prejudgment . . . considered to be intolerably high.”⁷⁶ There are certainly special facts and circumstances in this case that call into question the agencies’ ability to engage in unbiased decision-making.

43. The Commission has not explained what steps, if any, it has taken to ensure the public can have confidence in the impartiality of its decision. The Due Process Clause of the United States Constitution and the Commission’s governing statutes require recusal of the Chairman and any Commissioner or staff with a personal connection to the case that could implicate their impartiality, including status as a direct victim of unlawful conduct that could affect their impartiality.⁷⁷ The fact that senior current and former Commission leadership and high ranking personnel, as well as their families, were victims of MarioCop’s crimes no doubt angered the employees who investigated this matter, as well as the Chairman and Commissioners who voted to adopt this NAL. Indeed, as discussed further below, this anger may inform the accusatory tone of the NAL and its unprecedented fine—the calls hit close to home. And that anger is perfectly understandable. But acting as the judge, jury, and *victim* in the same case is at least one step too many. It raises the specter that the Commission may be acting in a biased manner. Even the *appearance* of personal animus threatens Telnix’s most basic constitutional and statutory rights.⁷⁸

44. The NAL thus violates Telnix’s right under the due process clause of the Fifth Amendment, which guarantees Telnix an impartial adjudicator.⁷⁹ “With respect to agency adjudicatory proceedings, due process might be said to mean at least ‘fair play.’ One of these essentials is the resolution of contested questions by an impartial and disinterested tribunal.”⁸⁰ Courts have explained that the “rigidity of the requirement that the trier be impartial and unconcerned in the result applies *more strictly* to an administrative adjudication where many of the safeguards which have been thrown around court proceedings have, in the interest of expedition and a supposed administrative efficiency been relaxed.”⁸¹ This right extends to both actual bias and the *appearance* of bias among the Commissioners and their staff. If a reasonable person would think that the FCC adjudicated this case differently because of its personal victimization, that is enough to violate Telnix’s due process rights.

⁷⁵ *Withrow v. Larkin*, 421 U.S. 35, 58 (1975).

⁷⁶ *Id.* at 57.

⁷⁷ *See, e.g.*, 5 C.F.R. § 2635.101(b)(8), (14); 47 C.F.R. § 19.735-102.

⁷⁸ *See* 5 C.F.R. § 2635.101(b)(14).

⁷⁹ *See Schweiker v. McClure*, 456 U.S. 188, 195 (1982) (“[D]ue process demands impartiality on the part of those who function in judicial or quasi-judicial capacities.”).

⁸⁰ *Amos Treat & Co. v. Sec. & Exch. Comm’n*, 306 F.2d 260, 263–64 (D.C. Cir. 1962).

⁸¹ *Helena Lab’ys Corp. v. Nat’l Lab. Rels. Bd.*, 557 F.2d 1183, 1188 (5th Cir. 1977) (emphasis added).

45. In agency adjudications, the remedy for bias (or the appearance of bias) is recusal or disqualification.⁸² When bias or the appearance of bias taints a proceeding, “the test for disqualification” is “whether ‘a disinterested observer may conclude that [the agency] has in some measure adjudged the facts as well as the law of a particular case in advance of hearing it.’”⁸³ It also explained that “an administrative hearing must be attended, not only with every element of fairness but with the very appearance of complete fairness.”⁸⁴

46. The Commission’s lack of impartiality is apparent in the NAL itself. The document spends more words describing MarioCop, who is not a party to this action, than it does Telnyx. In the factual background, the Commission begins by describing the conduct of MarioCop, not Telnyx.⁸⁵ And the NAL itself, as well as the Commissioners’ separate writings, focused on the apparent egregiousness of *MarioCop*’s conduct—not Telnyx’s alleged violation, which is the only matter before the Commission.⁸⁶

47. The need for recusal is compounded by the NAL’s failure to fully or candidly disclose how the agency’s decision-makers and advisors (and family members) were personally targeted and harmed by the unlawful calls of MarioCop, which would naturally generate feelings of outrage and color anyone’s ability to be impartial. The NAL stated only that “over a dozen” members of the Commission’s “staff” received calls. In theory, such a small group of affected persons might be able to recuse, and still permit the Commissioners to make an independent judgment. But by failing to disclose that commissioners, their chiefs of staff and legal advisors, and the front offices of the Enforcement Bureau and Office of General Counsel, among others, who received calls, the NAL obfuscates key facts of the investigation and explains why its impartiality is now at issue. A reasonable person would view the NAL’s effort to misleadingly shroud the magnitude of the apparent security breach as reason to question the Commissioner’s ability to judge the matter in an independent, unbiased manner.⁸⁷

48. In addition to fundamental standards of fairness as imposed by the Due Process Clause, the APA and the Commission’s governing regulations and statutes require recusal in this circumstance. For instance, the federal ethics rules, 5 C.F.R. § 2635.501-503, require recusal of a commissioner with a direct interest in a case. Moreover, the Commission has interpreted 47 C.F.R.

⁸² See *Cinderella Career & Finishing Sch., Inc. v. F.T.C.* 425 F.2d 583, 591 (D.C. Cir. 1970); see also, e.g., *In re AT&T, Inc.*, No. 202032170004, 2024 WL 1905227, at *26 (OHMSV Apr. 29, 2024); *In re Implementation of Section 309(j) of the Commc’ns Act*, 13 F.C.C. Rcd. 15920 (1998).

⁸³ *Cinderella*, 425 F.2d at 591 (quoting *Gilligan, Will & Co. v. SEC*, 267 F.2d 461, 469 (2d Cir. 1959)).

⁸⁴ *Id.* (emphasis added); see also *In re Implementation of Section 309(j) of the Commc’ns Act*, 13 F.C.C. Rcd. 15920 (“The courts have made clear that in an administrative adjudication ‘the appearance of bias or pressure may be no less objectionable than reality.’”) (quoting *ATX, Inc. v. United States Dep’t of Transp.*, 41 F.3d 1522, 1527 (D.C. Cir. 1994)).

⁸⁵ See generally Telnyx NAL.

⁸⁶ See *supra* note 1.

⁸⁷ See *In re AT&T, Inc.*, 2024 WL 1905227, at *26 (“What is relevant for purposes of evaluating bias in an adjudicatory proceeding is whether ‘a disinterested observer may conclude that [the agency] has in some measure adjudged the facts as well as the law of a particular case in advance of hearing it.’”).

§ 1.1 to embrace a duty to ensure its employees were not biased in their decision-making. That provision provides that the Commission “may on its own motion or petition of any interested party hold such proceedings as it may deem necessary ... in connection with the investigation of any matter which it has power to investigate under the law, or for the purpose of obtaining information necessary or helpful in the determination of its policies, the carrying out of its duties or the formulation or amendment of its rules and regulations.”⁸⁸ In a recent matter before the Commission, the Commissioners referred to this provision as allowing an investigation into “the impartiality of the Enforcement Bureau proceedings and the appearance of impartiality.”⁸⁹ Here, as discussed above, Commission employees—including Senate-confirmed voting members of the Commission—were targets of the alleged unlawful calling. There is no indication that affected persons were screened from the investigation or the Enforcement Bureau’s recommendations. Certainly the Commission must inquire as to their partiality.

49. Telnyx therefore requests recusal and/or disqualification of (a) any voting member of the Commission who directly received a call from MarioCop, (b) any Commission senior leadership and staff who received such a call, (c) any voting member of the Commission, senior leadership or staff whose family received a call and (d) any Commission employee who, based on their communications with or influence by those who were directly or indirectly targeted, cannot assure the public of the appearance of impartiality in the Telnyx proceeding. The votes of those personally affected must be rescinded. As a threshold matter, the voting members of the Commission who were impacted should immediately rescind their votes on the Telnyx NAL—and immediately cease participation in this matter. The Commission’s Inspector General should also conduct its own investigation into whether the Commission experienced a security breach that exposed personal cell phone numbers and if so, what steps the agency took and will take to contain contamination of personnel involved in the Telnyx enforcement proceeding.

III The Commission wrongly treats Telnyx’s one-way VoIP service as a Title II common carrier service.

50. The Commission alleges that Telnyx violated a single Commission rule: the Effective Measures rule.⁹⁰ This rule applies a net neutrality-like reinterpretation of the statutory text to expand the reach of Title II by one-way VoIP providers as if they were Title II “common carriers.” This reinterpretation of the Act was done without any statutory analysis and does not represent the “best read” of the Act.⁹¹ The Commission’s actions here are no more than a backdoor method to achieve a net neutrality-like policy objective: engaging in statutory reinterpretation as a means to impose Title II obligations on one-way VoIP providers. The Commission’s choice to enforce this rule without statutory support is surprising, as both Chairman Carr and Commissioner Simington strongly dissented in the Biden-era FCC’s decision to reinstate net neutrality based on

⁸⁸ 47 C.F.R. § 1.1.

⁸⁹ *In re Saturn Telecomms. Servs., Inc.*, 29 F.C.C. Rcd. 12520, 12530 (2014).

⁹⁰ 47 C.F.R. § 64.1200(n)(4).

⁹¹ See *Ohio Telecom Assoc. v. F.C.C.*, 124 F.4th 993 (6th Cir., 2025).

essentially the same interpretative sleight of hand. The Commission’s cited legal authority for the Effective Measures rule relies primarily on Title II’s “anti-discrimination” provisions:

Our legal authority to adopt these requirements stems from sections 201(b), 202(a), and 251(e) of the Communications Act of 1934, as amended (the Act), as well as from the Truth in Caller ID Act. Section 201(b) and 202(a) grant us broad authority to adopt rules governing just and reasonable practices of common carriers. While these rules are clearly within the scope of our section 201(b) and 202(a) authority, we find that it is essential that the rules apply to all voice service providers. Absent broad application, VoIP would remain a safe haven for bad actors.⁹²

51. In so doing, the Commission engages in questionable statutory reinterpretation without legal analysis. It was well established that the FCC cannot impose “common carrier-like” duties (i.e., the anti-discrimination provisions of Sections 201 and 202) on entities that are not classified as providers of Title II telecommunications services.⁹³ Indeed, courts have restricted the expansion of Title II obligations to non-Title II providers. *McDonnell Douglas Corp. v. Gen. Tel. Co. of Cal.*, 594 F.2d 720, 724-25 (9th Cir. 1979) (holding that the anti-discrimination provisions of Title II do not apply to a services provider when it provides a non-Title II service even if, in other contexts, it does provide services governed by Title II, explaining that “[w]e do not wish to unnecessarily expand the scope of federal jurisdiction in this area when it was the clear intent of Congress and other courts to limit that jurisdiction.”).

52. By asserting that the anti-discrimination provisions of the Act provide authority for applying the Effective Measures rule on one-way VoIP providers, the Commission repeats the same mistake that the DC Circuit overturned 11 years ago in *Verizon v. FCC*. Except this time, its mistake is *worse* because the Commission does not even facially attempt to defend this reinterpretation of the Act to classify one-way VoIP providers as Title II common carriers—it simply treats them as such to reach a policy objective – the very approach that led to the prenatal death of the Biden-era order to reinstate net neutrality.

53. While the Commission has previously argued that it had “ancillary jurisdiction” over Title I providers to impose certain provisions of Title II to Title I providers, it has never successfully imposed the anti-discrimination provisions of Sections 201 and 202 to one-way VoIP providers. Further, where a court did uphold the Commission’s authority to impose Title II obligations on certain non-Title II VoIP providers, the court expressly relied on *Chevron*’s now-defunct doctrine of agency deference to uphold the Commission’s statutory interpretation of its

⁹² *In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, 35 F.C.C. Rcd. 15221, 15233-34 (2020) (emphasis added).

⁹³ *Verizon v. FCC*, No. 11-1355 at 45-46 (D.C. Cir. 2014) (Tatel, J.) (“Given the Commission’s still-binding decision to classify broadband providers not as providers of “telecommunications services” but instead as providers of “information services,” such treatment would run afoul of section 153(51) [of the Act]: “A telecommunications carrier shall be treated as a common carrier under this [Act] only to the extent that it is engaged in providing telecommunications services.” 47 U.S.C. § 153(51))”

own authority.⁹⁴ But, *Loper Bright Enterprises* stripped federal agencies of the authority to adopt any interpretation that does not accord with the best meaning of the statutory text.⁹⁵ As the Sixth Circuit stated when it overturned the net neutrality rules, *Loper Bright* removed the Commission’s ability to assert new regulations based on ambiguous provisions not supported by the text of the statute, making clear that the ultimate power to interpret statutes governing federal agency authority lies with the courts.⁹⁶ The Sixth Circuit also correctly noted that the Act “favors light regulation under Title I” over Title II classification since “[w]ith the common-carrier designation comes significant regulatory oversight.”⁹⁷ Certainly, expansion of Title II status to VoIP services would not be the “best” interpretation of the underlying statutes.

54. In addition, the NAL compounds this misapplication of the law when it attempts to calculate the maximum forfeiture per violation.⁹⁸ It states that when Telnix applied for and was granted an international 214 authorization nearly 14 years ago, the Commission “authorized Telnix to become” a Title II common carrier.⁹⁹ The NAL concludes that this single authorization renders Telnix a common carrier under Title II, even in the context of one-way VoIP services.¹⁰⁰ But this backdoor, net neutrality-like reclassification should not be enforced by this Commission. As noted above, the test of whether one is a common carrier depends on the extent to which the provider operates as a common carrier. The Commission has never classified one-way interconnected VoIP as a Title II telecommunications service. Merely complying with a particular Title II-derived obligation does not reclassify a Title I service provider as a Title II service provider for all purposes. For example, a VoIP provider’s act of filing a FCC Form 499A with the Universal Service Administrative Company does not make it a Title II telecommunications carrier. It is surprising that this Commission would propose to enforce a discredited statutory interpretation in its first enforcement proceeding.

55. Lastly, any argument that the Commission relied on the TRACED Act as legal authority when promulgating the Effective Measures rule would be incorrect. In the *Fourth Report and Order*, the Commission expressly relied on the TRACED Act as authority for multiple rules, including the call blocking safe harbor when using reasonable analytics¹⁰¹ and call blocking redress

⁹⁴ See *Vonage Holdings Corp. v. F.C.C.*, 489 F.3d 1232 (D.C. Cir., 2007) (holding that imposing the Title II obligation to contribute to the universal service fund was a reasonable agency interpretation under *Chevron*).

⁹⁵ See *Loper Bright Enters. v. Raimondo*, 603 U.S. 369 (2024).

⁹⁶ *Ohio Telecom Assoc. v. F.C.C.*, 124 F.4th 993, 997-98 (6th Cir. 2025).

⁹⁷ 124 F.4th at 999.

⁹⁸ Telnix NAL at ¶20.

⁹⁹ *Id.*

¹⁰⁰ *Id.*

¹⁰¹ *In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, 35 F.C.C. Rcd. 15221, 15237 (2020).

mechanisms.¹⁰² The Commission expressly did not rely on the TRACED Act when adopting the Effective Measures rule.¹⁰³

IV Telnyx Met or Exceeded the Effective Measures Required by the Commission’s Rules.

- a Telnyx complied with the Effective Measures rule to prevent new and renewing customers from using its network to originate illegal calls.

56. The Effective Measures rule requires that voice service providers “[t]ake affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic.”¹⁰⁴ “Beyond that,” clarified the Commission, “we do not require that voice service providers take specific, defined steps, but instead permit them flexibility to determine what works best on their networks.”¹⁰⁵

57. The Telnyx NAL would find Telnyx liable for alleged violations based on a surprising rewriting of its Effective Measures rule. Even before *Loper Bright Enterprises*, the Seventh Circuit noted in *Kropp Forge* that a requirement to take “effective” measures does not provide “fair warning” that the agency actually requires regulated entities to conduct themselves according to a specific higher standard. This was also the holding of the Fifth Circuit in *Diamond Roofing*. There, the Court stated, a regulator must “state with ascertainable certainty what is meant by the standards [it] has promulgated.” And again:

“[A regulatee] is entitled to fair notice in dealing with his government. Like other statutes and regulations which allow monetary penalties against those who violate them . . . [the regulation] must give . . . fair warning of the conduct it prohibits or requires, and it must provide a reasonably clear standard of culpability to circumscribe the discretion of the enforcing authority and its agents.”¹⁰⁶

58. In *SmithKline Beecham*, the Supreme Court held that an agency should not receive deference when the agency’s interpretation of a regulation does not provide “fair warning” of the required conduct.¹⁰⁷ The Court continued: “Indeed, it would result in precisely the kind of ‘unfair surprise’ against which our cases have long warned.”¹⁰⁸ The Court in *SmithKline Beecham* also noted that “an agency should not change an interpretation in an adjudicative proceeding where

¹⁰² *Id.* at 15238, 15249.

¹⁰³ *See id.* at 15233.

¹⁰⁴ 47 C.F.R. § 64.1200(n)(4).

¹⁰⁵ *In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, 35 F.C.C. Rcd. 15221, 15232 (2020).

¹⁰⁶ *Diamond Roofing Co. v. Occupational Safety & Health Rev. Comm’n*, 528 F.2d 645, 649 (5th Cir. 1976).

¹⁰⁷ *Christopher v. SmithKline Beecham Corp.*, 567 U.S. 142, 156 (2012).

¹⁰⁸ *Id.*

doing so would impose ‘new liability ... on individuals for past actions which were taken in good-faith reliance on [agency] pronouncements’ or in a case involving ‘fines or damages.’”¹⁰⁹

59. One can look to the Commission’s reports and orders—the regulatory “preamble”—to the Effective Measures rule to define the word “effective.” As the D.C. Circuit has explained, “language in the preamble of a rule is a valid ‘source of evidence concerning contemporaneous agency intent,’ such that it can ‘establish rights and obligations or create binding legal consequences.’”¹¹⁰ The Effective Measures rule’s preamble attempts to clarify the regulation’s language, stating that the Commission expects only “affirmative, effective measures” to avoid fraudulent traffic, not “perfection.”

60. That choice to define the meaning of “effective” as excluding perfection has consequences. In issuing the regulation, the Commission conformed its view of what it means to have an “effective” program to that word’s ordinary definition: for a program to be “effective,” it must “[p]erfor[m] within the range of normal and expected standards.”¹¹¹ In other words, the Commission is bound by a definition of the word “effective” that specifically rejects a requirement of absolute perfection. The Commission instead chose a standard that required reasonable due diligence without further specificity of what that entailed. As a matter of basic logic and practicality, a robocall mitigation program can exercise reasonable due diligence, while still experiencing the occasional bad actor evading those controls.

61. In the NAL, the Commission chose to focus on whether a *program* is effective, not whether specific bad actors happen to (briefly) evade reasonable controls. But the Commission now acts on the new theory that because MarioCop briefly evaded Telnix’s controls, then those controls must have been ineffective. The binding language in the Effective Measures rule intentionally rejected the Commission’s interpretation in the NAL.

62. Although the specific text of subsection 64.1200(n)(4) does not itself define “effective,” the Commission issued a handful of other statements as part of the rule explaining how its terms should be understood. These statements, issued in the same rulemaking that went through notice-and-comment and published in the official agency record, form a part of the rule and are equally binding on the agency.¹¹² In those statements, the Commission was clear that it does not expect or require perfection, an impossible standard, from a provider’s Effective Measures. As the Commission noted (again and again):

- “Some commenters raise concerns that if steps are not universally or completely effective, voice service providers could face liability despite best efforts or that, if extensive measures are required, small voice service providers may be unable to satisfy this requirement. We make clear that we do not expect perfection; particularly clever bad actors may, for a time, evade detection. In these cases, a

¹⁰⁹ *Id.* at 156-57 (citing *Nat’l Lab. Rel. Bd. v. Bell Aerospace Co.*, 416 U.S. 267, 295 (1974)).

¹¹⁰ *Duke Energy Progress, LLC v. FERC*, 106 F.4th 1145, 1154 (D.C. Cir. 2024) (cleaned up).

¹¹¹ Black’s Law Dictionary (12th ed 2024).

¹¹² *See Duke Energy*, 106 F.4th at 1154.

voice service provider could exercise its contractual remedies or take additional mitigation steps. If the voice service provider takes these steps and does not originate a significant amount of illegal traffic, it satisfies the rules we adopt today.¹¹³

- “We agree with the commenters that urge us to give voice service providers flexibility.”¹¹⁴
- “For example, in establishing affirmative obligations for voice service providers, we ensured that voice service providers have flexibility to determine how best to comply and made clear that we do not expect perfection.”¹¹⁵
- “The Report and Order makes clear that, while we do not define specific steps, we do not expect perfection[.]”¹¹⁶
- “Voice service providers can comply in a number of ways, so long as they know their customers and take measures that have the effect of actually restricting the ability of new and renewing customers to originate illegal traffic. Flexibility reduces the burden on voice service providers.”¹¹⁷
- “Different call patterns may require different approaches, and methods that are appropriate for one voice service provider may not be the best for others.”¹¹⁸
- “Flexibility to adapt to changing calling patterns is necessary to avoid giving the ‘playbook’ to bad actor callers, thus an outcomes-based standard is most appropriate.” (Emphases added).¹¹⁹

63. It makes no difference that the regulation specifies the need to implement effective measures “*including*” knowing your customer.¹²⁰ Based on the Commission’s own statements, the

¹¹³ *In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, 35 F.C.C. Rcd. 15221, 15233 (2020) (emphasis added).

¹¹⁴ *Id.* (emphasis added).

¹¹⁵ *Id.* at 15268 (emphasis added).

¹¹⁶ *Id.* at 15260 (emphasis added).

¹¹⁷ *Id.* at 15233 (emphasis added).

¹¹⁸ *Id.* (emphasis added).

¹¹⁹ *In re Advanced Methods to Target & Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, 38 F.C.C. Rcd. 5404, 5423 (2023) (emphasis added). The Commission also declined to adopt a Effective Measures certification requirement of VoIP providers. 38 F.C.C. Rcd. 15404, 5424-25. (“The VoIP Direct Access Further Notice sought comment on whether to require direct access applicants to certify that they ‘know their customer’ through customer identity verification. After considering the record, we decline to adopt a specific know-your-customer certification at this time.”) *In re Numbering Policies for Modern Commc’n*, Second Report and Order, FCC 23-75 ¶¶ 58 (Sept. 22, 2023), <https://docs.fcc.gov/public/attachments/FCC-23-75A1.pdf>.

¹²⁰ 47 C.F.R. § 64.1200(n) (emphasis added).

Commission clearly does not expect that a provider will infallibly know every customer; instead, a provider's Effective Measures must be broadly "effective" with the knowledge that "bad actors may . . . avoid detection." It would be absurd if the rule allowed for subjective, flexible "affirmative, effective measures" but strict liability for a supposed "Effective Measures" obligation that has to do with knowing a customer. As the Supreme Court held in *United States v. Brooks-Callaway Co.*, "the adjective . . . must modify each event set out in the 'including' phrase. Otherwise absurd results are produced."¹²¹ That means that the Commission cannot rely on the regulation's use of the word "including" to expand the reach of the rule beyond what it plainly requires—"effective" measures, not perfection.

64. Misapplying those fundamental rules of statutory interpretation, the Telnyx NAL asserts that the Commission's "rules require Telnyx to know its customers. Yet it did not know who the MarioCop Account holders were." But, just as the Supreme Court warned in *Brooks-Callaway Co.*, the absurdity of defining "including" without reference to the other obligations specified in a list becomes apparent when applied to other contexts. For example, the Commission issued a press release that lauded its Robocall Response Team for "getting results" because of a "99% drop in auto warranty scam robocalls after an FCC action" and an "88% month-to-month drop in student loan scam robocalls."¹²² Based on the Commission's logic, neither of these results was "effective" since they did not reduce either auto warranty or student loan scam calls by 100%. But, in fact, the Commission's measures were effective. And so are Telnyx's Effective Measures that result in 99.8% of its customers never being associated with a traceback.¹²³

65. The Commission has also clarified repeatedly that the expectations discussed above specifically refer to providers' Effective Measures *programs*. In other words, the Commission has stated that what it means to have an "effective" program looks to the policies and procedures implemented by the program as a whole. The "effective" adjective applies equally to "prevent[ing] new and renewing customers from using its network" and the obligations to know one's customers and exercise due diligence. A single caller's temporary evasion of those controls does not mean the program is insufficient. First and most obviously, this interpretation echoes the opinions of then-Commissioner Carr and Commissioner Simington in the Lingo Telecom NAL.¹²⁴ Second, this interpretation is confirmed by multiple Commission rulemakings. In the *Gateway Provider Order*, for example, the Commission clarified that, like for originating providers, the Commission adopted a "flexible approach to know-your-customer requirements, rather than specific mandates" and elected to grant gateway providers "the flexibility to determine the exact measures to take . . .

¹²¹ 318 U.S. 120, 123 (1943).

¹²² FCC Adopts New Rules to Close the 'Lead Generator' Robocall and Robotexts Loophole and Facilitate Blocking of Unwanted Robotexts, Press Release (Dec. 13, 2023), <https://docs.fcc.gov/public/attachments/DOC-399082A1.pdf>.

¹²³ See Declaration of David Casem, para. 21 ("Exhibit A").

¹²⁴ See, e.g., Lingo Telecom NAL, p. 20 (Comm'r Simington Statement) (noting that "it's not actually clear what their [Effective Measures] obligations now are" and admitting that contractual commitments are enough to know one's customer under the rule).

consistent with our existing requirement for originating providers[.]”¹²⁵ Subsequently, when the Commission extended the Effective Measures rule to all voice service providers, the Commission again clarified that, in the context of knowing one’s customers, it “do[es] not expect perfection.”¹²⁶

66. In fact, the Commission strongly intimated that contractual provisions alone are enough to satisfy providers’ requirements. The Commission stated, “While more involved investigations represent some burden, particularly for smaller voice service providers, voice service providers of all sizes should be able to impose and enforce relevant contract terms.”¹²⁷ The Commission goes on to say, “The Report and Order requires voice service providers to respond to (i) traceback [sic], (ii) mitigate illegal traffic when notified of such traffic by the Commission, and (iii) take affirmative steps to prevent illegal calls from new and renewing customers . . . The *Report and Order* makes clear that, while we do not define specific steps, we do not expect perfection, and that enforcement of contract clauses is sufficient to satisfy the third requirement.”¹²⁸

67. If enforcement of contractual clauses is sufficient to satisfy the “affirmative, effective measures” requirement, and the “affirmative, effective measures” requirement includes the KYC requirement, then enforcement of contractual clauses is wholly sufficient. This was the position of then-Commissioner Carr and Commissioner Simington in the Lingo Telecom NAL. There, Commissioner Simington emphasized that point:

Lingo states in its defense that it relied on Life Corp.’s contractual statements about numbers and permissions in what the Enforcement Bureau notes was a one-page form with no diligence backing it up. This might not be the most sympathetic defense, but it isn’t an unreasonable one, because the FCC has never required a higher standard. This is why the FCC has to have recourse to vague statements like “reasonable KYC [know your customer] protocols,” and needs to make a novel finding that a “generic, blanket, check-the-box ‘agreement,’” is insufficient, in order to find liability.¹²⁹

68. As noted above, the Commission made a number of consequential decisions in issuing the Effective Measures rule. Most importantly, though it refused to provide guidance despite requests to do so from industry. The regulatory preamble is clear that the Commission’s interpretation of the rule in the Telnix NAL is a novel reinterpretation of the Effective Measures rule without prior notice. In apparent recognition that the constant evolution of bad actors’ schemes would make specific requirements or prohibitions functionally impossible (and that bad actors inevitably will sometimes evade Effective Measures programs), the Commission assured regulated

¹²⁵ *In re Advanced Methods to Target & Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, Sixth Report and Order, FCC 22-37, ¶¶ 98-99 (May 19, 2022) (“Gateway Provider Order”), <https://docs.fcc.gov/public/attachments/FCC-22-37A1.pdf>.

¹²⁶ *In re Advanced Methods to Target & Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, Seventh Report and Order, FCC 23-37, ¶¶ 49-50 (May 18, 2023), <https://docs.fcc.gov/public/attachments/FCC-23-37A1.pdf>.

¹²⁷ *In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, 35 F.C.C. Rcd. 15221, 15233 (2020).

¹²⁸ *Id.* at 15260 (romanettes added for clarity) (emphasis added).

¹²⁹ Lingo Telecom NAL, p. 20 (Comm’r Simington Statement).

industry over and over again that “perfection” would not be required—only reasonable measures. The Commission is bound by those pronouncements, and industry is entitled to rely on them, at least until such time as the Commission conducts a notice and comment rulemaking proceeding to clarify or amend the Effective Measures rule.

69. Even so, Telnyx does perform to a “higher standard” than these regulations facially require and has long viewed its fraudulent-traffic mitigation program as a valuable service of its business. Telnyx’s Effective Measures include (i) requiring that its customers first adopt Telnyx’s Terms of Service, Privacy Policy, and Acceptable Use Policy, the latter of which prohibits using the services for “illegal, improper, and/or inappropriate purposes”; (ii) requiring that customers register with a business email address, physical location address, and business name (if applicable); (iii) tracking all customers’ IP addresses to prevent banned customers from re-registering; (iv) tracking all customers’ payment methods, scanning all payments for potentially suspicious patterns, (v) utilizing Braintree, a third-party fraud monitoring service and subsidiary of PayPal, to continually monitor payment methods with built-in anti-fraud measures; and (vi) employing an industry-recognized, agnostic, third-party fraud decisioning platform managed by Sift.¹³⁰ Sift scans customer credentials to ensure they are not associated with (a) blacklisted IP addresses, (b) blacklisted countries, (c) blacklisted words in email names, (d) blacklisted account names, (e) new and repeated email addresses, (f) disposable domains, or (g) other fraud indicators that lead Sift to determine the account has a high potential for abuse. Sift then, using its proprietary fraud detection algorithm, aggregates these factors together and provides a “score” for each customer. Score low enough and the customer is automatically blocked at signup before they can send a single call. Score above the threshold but still within a margin of error and Telnyx will monitor that customer’s outbound traffic for suspicious activity.

70. Telnyx uses STIR/SHAKEN to record both the identity header details and verification outcomes of customers’ traffic by downstream providers for analysis and monitoring purposes.¹³¹ Telnyx subjects all Telnyx-originated traffic to continuous monitoring, including monitoring of all IP addresses associated with blocked accounts and accounts that share domain names with suspended accounts.¹³² Telnyx also employs internal tools to examine the traffic metrics of all customers on an ongoing basis to detect fraudulent activity instantaneously, including monitoring for (i) excessively short average call duration rates, (ii) suspicious answer seizure ratios (i.e., the percentage of successfully connected calls relative to the number of attempted calls), and (iii) a high number of simultaneous active calls from a single account. Accounts less than two months old that display any of these patterns are immediately blocked.¹³³ Telnyx performs daily routine script executions to detect newly registered users whose Calling Line Identification (“CLI”) display names include potentially suspicious keywords.¹³⁴

¹³⁰ See Exhibit A, ¶ 10.

¹³¹ See *id.* ¶ 11.

¹³² *Id.*

¹³³ *Id.*

¹³⁴ *Id.*

71. Telnyx employs robust call origination and number verification policies and procedures. Telnyx validates a customer’s origination number against an international Do Not Originate list to prevent misuse and checks origination numbers against Nomorobo, a third-party database of known fraudulent numbers used by the Enforcement Bureau, to block potential threats.¹³⁵ For U.S. domestic outbound calls, Telnyx (i) verifies the existence of an appropriate Local Routing Number (LRN) and blocks calls with non-existent LRNs, and (ii) does not allow calls with invalid CLIs to exit the Telnyx network. Non-Telnyx numbers intending to originate traffic from the Telnyx network are required to undergo number verification to prevent spoofing (i.e., the display of inaccurate caller ID information).¹³⁶

72. Lastly, Telnyx onboards all customers as “Level 1” (i.e., limited access) account holders, which includes significant limitations on available calling functionalities and global outbound calling limits, specifically ten simultaneous calls.¹³⁷ To reach “Level 2” (i.e., full access) status, customers must undergo rigorous additional fraud detection and call pattern review. Unless stated otherwise, the due diligence described above applies to both Level 1 and Level 2 customers.¹³⁸

73. Following the MarioCop incident, Telnyx acted quickly on its own initiative to install even more advanced measures.¹³⁹ Telnyx chose to implement these measures due to its commitment to ensuring the integrity of our services and being an industry leader in fraud prevention; Telnyx was not instructed to do so by the Commission or any other government authority.¹⁴⁰ In March 2024, Telnyx began collecting credit card information before allowing customers to create an account. Based on the credit card information plus other account information, Sift creates credit card risk profiles for each customer.¹⁴¹ If Sift indicates an account is high risk, then Telnyx will require that account to be further verified by Onfido, a photo-based digital identity platform.¹⁴² Onfido requires that such customers provide multiple-angle photographs for identity verification. In April, Telnyx restricted the use of PayPal as a payment method to only Level 2 accounts.¹⁴³ In May, Telnyx began requiring that all new accounts provide government-issued ID (this had previously only applied to accounts seeking Level 2 status) and instituted heightened monitoring for a customer’s first 72 hours on the network.¹⁴⁴ Finally, in July, Telnyx began restricting the use of Bitcoin as a payment method to only Level 2 accounts.¹⁴⁵ These

¹³⁵ *Id.*, ¶ 12.

¹³⁶ *Id.*

¹³⁷ *Id.*, ¶ 13.

¹³⁸ *Id.*

¹³⁹ *Id.*, ¶ 17.

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

¹⁴² *Id.*

¹⁴³ *Id.*

¹⁴⁴ *Id.*

¹⁴⁵ *Id.*

steps are not specifically required by the Commission, but Telnyx implemented them in the interest of furthering the goal of robocall mitigation.

74. Telnyx is also an established leader amongst VoIP service providers with a demonstrated commitment to—and vested interest in—preventing unlawful traffic.¹⁴⁶ Telnyx was a longstanding Supporting Partner of the ITG, providing support and guidance to the sole consortium selected by the FCC to conduct call traceback efforts.¹⁴⁷ Telnyx is also an active participant in the North American Numbering Council’s (NANC) CATA Working Group and NAOWG, contributing its expertise to the ongoing development of numbering policies that enhance the security and integrity of the telecommunications ecosystem.¹⁴⁸ The CATA Working Group focuses on the technical and policy aspects of call authentication, particularly in the fight against illegal robocalls.¹⁴⁹ Meanwhile, the NAOWG oversees the operational aspects of numbering, addressing issues such as number use, reclamation, and resale to mitigate potential abuse, misuse, and disuse within the numbering system.¹⁵⁰ In these capacities, Telnyx has often worked directly with the Commission and industry to publish reports on fraud and illegal robocall prevention.

75. Telnyx was instrumental in drafting responses to two charge letters issued by the Commission to CATA and NAOWG in 2024.¹⁵¹ CATA, in particular, addressed multiple topics related to direct access to numbering resources, with a focus on preventing fraud and illegal robocalls. CATA examined the impact of number rotation and “snowshoeing” techniques as well as the use of U.S. North American Numbering Plan (NANP) numbers for international call origination, which can be exploited by fraudsters. Telnyx led the charge of examining the potential abuse of trial numbers, proposing best practices to prevent misuse while maintaining legitimate access.¹⁵² Telnyx also assisted in creating the “Best Practices for the Implementation of Call Authentication Frameworks” (“CATA Report”) in 2020 at the request of the Commission.¹⁵³

76. Telnyx has always been deeply committed to promoting best practices within the communications industry and mitigating illegal traffic. In addition to NANC and its CATA Working Group and NAOWG, and (prior to this enforcement action) the ITG, Telnyx also participates in the following industry organizations and working groups:

¹⁴⁶ *Id.*, ¶ 5.

¹⁴⁷ *Id.*, ¶ 5.

¹⁴⁸ *Id.*, ¶ 6.

¹⁴⁹ *Id.*

¹⁵⁰ *Id.*

¹⁵¹ *See id.*

¹⁵² *See id.*

¹⁵³ *See generally* NANC Call Authentication Trust Anchor Working Group, *Best Practices for the Implementation of Call Authentication Frameworks* (Sep. 24, 2020) (hereinafter “CATA Report”),

<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>.

- NAPM LLC (North American Portability Management), which oversees the contracts for the LNP administrators;
- CIC (Carrier Identification Code Administration), which manages the assignment and administration of carrier identification codes used for routing and billing in telecommunications networks;
- SAC (Service Access Codes Administration), which administers codes that provide access to specific services, ensuring proper allocation and management;
- NTAC (Network Testing and Automation Committee), which focuses on developing and promoting testing methodologies and automation tools to enhance network reliability and performance;
- NICC (Network Interoperability Consultative Committee), which develops interoperability standards to ensure seamless communication across different networks and services in the UK;
- Future Voice Architecture (FVA), which explores and defines the evolution of voice services architecture, focusing on next-generation technologies and protocols;
- ATIS IPNNI/PTSC (IP Network-to-Network Interface / Packet Technologies and Systems Committee), which develops standards for IP network interconnections and packet-based technologies to ensure interoperability and security;
- INCOMPAS and INCOMPAS Robocalling, which represent competitive communications companies and advocates for policies to combat robocalling and enhance consumer protection;
- NG 6G (Next Generation 6G), which focuses on research and development of sixth-generation (6G) mobile network technologies, aiming to define future standards and applications;
- Blocking and Labeling Working Group (US Telecom), which develops strategies and best practices for identifying, blocking, and labeling unwanted robocalls to protect consumers;
- ATIS NGIIF (Next Generation Interconnection Interoperability Forum), which addresses operational aspects of next-generation network interconnection to ensure seamless interoperability between service providers;
- VON (Voice on the Net Coalition), which advocates for policies that promote the growth and innovation of internet voice communications;

- ATIS IP Interconnection Task Force, which focuses on establishing standards and agreements for IP-based network interconnections to ensure seamless data and voice transmission;
- Somos Public Policy Consortium, which collaborates on public policy initiatives related to numbering and routing to enhance telecommunications services;
- ATIS INC (Industry Numbering Committee), which develops guidelines and recommendations for numbering resource administration to promote efficient number utilization; and
- CIGRR (Carrier Identification Code Guidelines Review Group), which reviews and updates guidelines for the assignment and management of Carrier Identification Codes.¹⁵⁴

77. The Commission stated that providers who exercise their contractual clauses and do not originate a significant amount of illegal traffic “satisf[y] the rules we adopt today.”¹⁵⁵ Telnix does not originate a significant amount of illegal traffic, and the Commission has never alleged as much; therefore, Telnix fully satisfies the Effective Measures rule.

b *The Telnix NAL’s other miscellaneous arguments fail.*

i *Telnix does not allow “high volume” traffic.*

78. The Telnix NAL argues that Telnix’s policy of allowing 10 simultaneous calls from Level 1 (i.e., trial) accounts enabled high-volume calling, and “the Commission has explained that greater KYC measures are needed when a prospective customer is applying to use services that will allow the origination of a high volume of calls . . . [and] voice service providers may extensively investigate new customers seeking access to high-volume origination services”¹⁵⁶ Though Telnix already does use enhanced Effective Measures for customers seeking to originate a high volume of traffic (those with Level 2 accounts), we note that this characterization is not accurate, as the Commission did not say greater KYC measures “are needed,” merely that such measures are “recommend[ed].”¹⁵⁷ Furthermore, when the Commission stated that providers “may” extensively investigate those seeking the ability to make high-volume calls, it did so in the context of assuring providers that they had flexibility to pick and choose the practices and procedures that worked best for their network.¹⁵⁸

79. As noted above, Telnix allows Level 1 accounts to place up to 10 simultaneous calls. Anything more requires that the customer apply for a Level 2 account. The additional

¹⁵⁴ See Exhibit A, ¶ 6.

¹⁵⁵ *In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, 35 F.C.C. Rcd. 15221, 15234 (2020).

¹⁵⁶ Telnix NAL, ¶ 11.

¹⁵⁷ *In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, 35 F.C.C. Rcd. 15221, 15232 (2020).

¹⁵⁸ *Id.* at 15233.

Effective Measures used during the Level 2 vetting process are proprietary, but they are extremely strict and include the use of age verification, government-issued ID, and substantial facial recognition technology.

80. The Commission does not explain in the Telnix NAL (nor has it ever stated elsewhere) what it believes constitutes allowing transmission of “high volume” traffic. It appears the Commission is reserving the right to apply that label on an *ad hoc* basis, as it does for alleged Effective Measures violations. But Telnix’s 10-call-limit (i) complies with NANC best practices,¹⁵⁹ and (ii) is industry standard for residential and small business customers. By brief example, CenturyLink offers a business bundle of up to 10 lines and a “volume” bundle of more than 10 lines.¹⁶⁰ CenturyLink also offers an additional “business line volume” plan of 50 or more lines,¹⁶¹ local business voice plans for up to 19 employees,¹⁶² and voice plans for medium businesses from 20-500 employees.¹⁶³ Likewise, T-Mobile offers small business plans with up to 12 lines,¹⁶⁴ and Vonage offers “small business” plans for up to 48 employees.¹⁶⁵ SignalWire allows one call per second per number from unlimited numbers.¹⁶⁶ RingCentral’s desktop and web app allows up to six concurrent calls and their desktop phone allows up to 10 concurrent calls.¹⁶⁷ Different providers have different plans, but 10 concurrent calls is consistent with industry standards for basic plans.

81. The Commission’s past enforcement actions are illustrative of what it believes are “high volume” calling campaigns. Telnix has reviewed every major robocalling enforcement action of TCD over the past seven years: Abramovich (2018), Roesel (2018), Moser (2020), Rising Eagle (2021), Rhodes (2021) Robbins – NAL (2022), Burkman (2023), Sumco Panama (2023), Dorsher (2023), Kramer (2024), Lingo Telecom (2024), and now, Telnix – NAL (2025). MarioCop completed 1,117 apparently illegal calls. Prior to the Telnix NAL, the Commission had

¹⁵⁹ Fed. Commc’ns Comm’n, *Report on Direct Access to Numbers by Interconnected Voice over Internet Protocol (VoIP) Providers*, § 2.5.6 (Dec. 13, 2024), <https://www.fcc.gov/files/cata-direct-access-report-12-13-24>.

¹⁶⁰ See Qwest Corporation d/b/a CenturyLink, QC Exchange and Network Services Tariff, at 476, 480, 490 (Jan. 29, 2025), <https://www.edockets.state.mn.us/documents/%7B303EB494-0000-C71A-87B4-DE39FD99DEA2%7D/download?contentSequence=0&rowIndex=52>.

¹⁶¹ *Id.*

¹⁶² See *CenturyLink Simply Unlimited Business Internet Services*, CenturyLink, <https://www.getcenturylink.com/centurylink-business> (last visited Feb. 25, 2025).

¹⁶³ *Id.*

¹⁶⁴ *Unlimited small business plans for all your devices*, T-Mobile, https://www.t-mobile.com/business/plans/small-business-unlimited-data-plans?icid=TFB_TMO_P_TFBDATAMAC_XJOVV49PL81NS259L34577 (last visited Feb. 25, 2025).

¹⁶⁵ *VBC Plans and Pricing*, Vonage, <https://www.vonage.com/unified-communications/campaigns/small-business-communications/plans-and-pricing/> (last visited Feb. 25, 2025).

¹⁶⁶ Susan Russell, Common Voice FAQs, SIGNALWIRE (Aug. 2022), <https://forum.signalwire.community/t/common-voice-faqs/68>.

¹⁶⁷ RingCentral Support, *Allowing agents to handle multiple calls in a RingEX call queue*, https://support.ringcentral.com/article-v2/Allowing-agents-to-handle-multiple-calls-in-a-RingEX-call-queue.html?brand=RingCentral&language=en_US&product=RingEX&utm (last visited Feb. 12, 2025).

never alleged a “high volume” calling campaign with fewer than over 47,000 calls (and the next closest to that was 21,000,000 calls). Using these enforcement actions, we created Table 1 below to illustrate the point that the Commission’s vague reference to “high-volume” traffic in the NAL is not supported by the term’s use in describing the traffic of prior enforcement actions:¹⁶⁸

Table 1: FCC Robocall High Volume Comparison

Order Short Name	Total Calls	Calls per Day	“High volume”	Language used
Abramovich	96,758,223	1,075,091	Yes	“Massive volume”
Roesel	21,000,000	233,333	Yes	“Large volume”
Moser	47,610	23,805	Yes	“Large-scale”
Rising Eagle	1,000,000,000	7,407,407	Yes	“Large volumes”
Rhodes	4,959	23	No	—
Robbins (NAL)	514,467	16,596	No	—
Burkman	1,141	—	No	—
Sumco Panama	5,000,000,000	55,555,556	Yes	“Large volume”
Dorsher	9,763,599	162,727	No	—
Kramer¹⁶⁹	9,581	9,581	No	—
Lingo (NAL) Lingo (CD)	3,978 ¹⁷⁰	3,978	No	—
Telnyx	1,797 ¹⁷¹ 1,117	1,797 1,117	Yes	“High volume”

82. Unlike in Abramovich, Roesel, Rising Eagle, Robbins, Sumco Panama, and Dorsher, it is not possible for Telnyx customers to place such a high volume of calls. Put simply: Telnyx does not enable high-volume, short-duration calling through its application programming

¹⁶⁸ See FCC Robocalling Enforcement Action Table (created Feb. 8, 2025) (“Exhibit F”).

¹⁶⁹ The Kramer Forfeiture Order does refer to Kramer’s conduct as “mass-spoofing,” but these reflect two separate concepts: on the one hand is the volume of traffic and on the other hand is the amount of numbers that a Truth in Caller ID Act violator spoofs. It is very possible to have a “mass-spoofing” campaign without sending a high volume of calls. But even if the Commission were to argue that these concepts are analogous, that just speaks to how useless the concept of “high volume” is that it can simultaneously refer to 1,000 or 9,000 calls or 5 billion calls. Its hackneyed use by the Commission leaves it effectively meaningless.

¹⁷⁰ FCC stated there was a total number of 9,581 calls with 3,978 of them originating from Lingo. If calculated using the total number of calls, the fine per call comes to \$208.75. See Lingo Telecom NAL, ¶¶ 9, 28.

¹⁷¹ 1,797 reflects the number of non-completed calls. 1,114 reflects the number of completed calls.

interface (API). If Telnyx did see a suspicious spike in traffic, it would be flagged for blocking by Telnyx’s robocall mitigation measures.

ii Telnyx’s Effective Measures were then, and are now, compliant.

83. The Telnyx NAL mistakenly concludes that Telnyx’s Effective Measures compliance was “essentially ineffective” because one bad actor escaped detection.¹⁷² But that conclusion impermissibly makes strict liability the standard, rather than effective mitigation. The Commission’s caricature of the effectiveness of Telnyx’s Effective Measures is also factually baseless. Telnyx’s Effective Measures are very effective—demonstrably so. In 2024, Telnyx blocked tens of thousands of attempted new customer signups. In fact, Telnyx’s measures are so stringent that it blocked a full 49.5% of all attempted new customer signups.¹⁷³ In other words, almost half of all potential customers are blocked due to insufficient identification before they can place a single call. And when potential customers cannot access Telnyx’s network, they simply go elsewhere to competitors with less stringent fraud prevention requirements. Telnyx receives daily complaints from apparently “good actors” about its onerous fraud prevention policies, which prevent those potential customers from establishing accounts on the Telnyx platform, ultimately costing Telnyx customers and revenue.¹⁷⁴

84. Telnyx’s low rate of tracebacks is further evidence of its strong measures. In 2024, Telnyx had 37,722 active customers, but in the last year only 73 unique customers had a traceback associated with their account.¹⁷⁵ Even assuming *arguendo* that every traceback identifies a bad actor, that means at minimum 99.8% of Telnyx’s customers are never implicated in any form of robocall investigation. If 99.8+% is not effective enough to show that Telnyx “ensur[es] that its services are not used to originate illegal traffic,” then what is?

85. The Commission’s decision to refer to Telnyx’s vetting processes as “ineffective” shows the Commission’s lack of familiarity with the subject matter of this enforcement action: fraud mitigation. Sift, whom Telnyx employs to assess the fraud risk of its prospective customers, possesses over 40 patents, has overseen 1 trillion unique identification events, and has over 12 years of industry experience. G2, a leading software marketplace, recognized Sift with both its Momentum Leader Award and Enterprise Leader Award for Winter 2024. Even more impressive, Forrester Research, the industry-leading, publicly traded global market research company, named Sift a Wave™ Leader, Digital Fraud Management, in 2023. Forrester extensively compared the top 15 digital fraud management vendors on the market and concluded that Sift had the second strongest current product offering. Of the 15 vendors, Sift was one of only two to be named a market “Leader.” Forrester says of Sift:

Sift’s solution has grown from a retail-focused, card payment fraud management tool for merchants into a complete fraud management solution that now covers

¹⁷² Telnyx NAL at ¶14.

¹⁷³ *See id.* ¶ 21.

¹⁷⁴ *See id.* ¶ 12.

¹⁷⁵ *See id.* ¶ 21.

cryptocurrency and alternative, peer-to-peer (P2P) payments. Sift has a differentiated technical roadmap, a disproportionately large user group, and above-average internal processes to ensure and maintain its solution's customer adoption. . . Sift provides outstanding productized rules and risk-scoring strategies for various payment types as well as for non-payment activities like new account opening, return and promotion fraud, and content abuse.¹⁷⁶

86. A contract with Sift is far and away the industry standard for fraud mitigation and customer screening. Apart from Telnyx, other Sift fraud mitigation customers include Twilio, Shopify, Box, Rocket Money, Yelp, Reddit, Nikon, Hertz, Zipcar, Everlane, Harry's, OkCupid, Skill Share, Poshmark, Rently, Patreon, Seat Geek, Shutterstock, Zillow, Fanduel, Underdog Fantasy, Couchsurfing, Doordash, and many other companies who require strong fraud detection programs. To deliver its anti-fraud services, Sift partners with numerous industry-leading brands, including Google Cloud Marketplace, Google Big Query, Amazon Redshift (an AWS product), Stripe, Ekata (a MasterCard company), Zendesk, Telesign, and Onfido.

87. As noted above, in addition to receiving Sift's risk score, Telnyx then continues to monitor new accounts for potential red flags and acts swiftly to shut down illegal traffic. No Effective Measures are perfect, but Telnyx's measures are effective. The Commission does not have to take Telnyx's, Sift's G2's, or Forrester's word for it because Telnyx in fact blocks so many customers who fail its identification requirements that this is a major source of Telnyx's customer complaints. Below are just a few of the one-star and two-star reviews Telnyx has received from aggrieved customers blocked by its Effective Measures compliance program:

- "Request of documents that borderlines identity theft. I made the account, which was blocked immediately after I confirmed my e-mail. I wasn't able to login or do any actions so I was surprised when I saw that my account was locked 1 second after confirming my e-mail. What could I have done since I was not able to login not even once?"¹⁷⁷
- I found Telnyx to be very difficult to use. KYC on sign-up including ID, face scan via app. Account locked upon sign upflow completion. A sales rep had to unlock it for me. Another round of KYC to add a payment method. A few days into testing the account was locked again. I decided to not port my numbers in.¹⁷⁸
- "Unable to sign up. They blocked my account immediately when I attempted to verify via email."¹⁷⁹

¹⁷⁶ Andra Cser, et al., The Forrester Wave™: Digital Fraud Management, Q3 2023, FORRESTER (Aug. 29, 2023), <https://reprints2.forrester.com/#/assets/2/2526/RES178506/report>.

¹⁷⁷ Customer complaint available at <https://www.trustpilot.com> (last visited Feb. 26, 2025) ("Exhibit D").

¹⁷⁸ Customer complaint available at <https://www.ycombinator.com> (last visited Feb. 26, 2025) ("Exhibit E").

¹⁷⁹ Exhibit D.

- “I created a business account for our company, ordered a phone number, verified my identity via Onfido and submitted all the verification documents they asked for . . . and few hours later blocked our account during the verification process without any reason[.]”¹⁸⁰
- “Created an account and purchased some credits to implement the Messaging API. Account was blocked automatically by the system - no reason given. I used a credit card that matches my name, and I registered with my company email.”¹⁸¹

88. Losing some potential customers who fail identification screening or other measures is a risk Telnix is willing to take to ensure the integrity of its services and the calls placed on its network. But there can be no dispute that its measures screen out a significant amount of those attempting to become customers.

89. Ultimately, the Commission’s actions will significantly chill industry’s ability to experiment with and implement new anti-fraud technologies. E.O. 14219 requires that agencies not “harm the national interest by significantly and unjustifiably impeding technological innovation.”¹⁸² In the *Seventh Report and Order*, the Commission expressly stated that industry needed “[f]lexibility to adapt to changing calling patterns.”¹⁸³ But a strict liability standard sprung on industry incentivizes companies to not innovate and not adapt to those changing calling patterns. Why would any company employ an AI-related fraud detection service if the Commission applies a strict liability standard? If an AI service screens out 99.9% of attempted fraudulent customers of a platform, the Telnix NAL suggests that the Commission will come after the platform for the 0.1% who get by. No one would innovate under those conditions. To expect perfect performance from emerging technologies is not sound policy, and it will wreak havoc on the Administration’s explicit policy goals of encouraging technological innovation.

90. Furthermore, the Commission’s surprising pivot to strict liability presents industry with a Hobson’s choice. Even before this action, industry needed to balance the competing aims of an effective fraud mitigation program and a functional user experience: implement policies that are too stringent and legitimate customers will complain, then possibly give up and go to other platforms; become too lax and the provider risks onboarding bad actors, eroding public confidence, also costing the provider revenue, and inviting private litigation or enforcement actions. Neither is desirable. The Effective Measures rule and its regulatory preamble show the Commission once understood that tension and offered a clear path. But this regulation by enforcement would require all providers use the most stringent possible fraud mitigation measures, regardless of the cost to

¹⁸⁰ Exhibit D.

¹⁸¹ Exhibit D.

¹⁸² White House, *Ensuring Lawful Governance and Implementing the President’s “Department of Government Efficiency” Regulatory Initiative* (Feb. 19, 2025), <https://www.whitehouse.gov/presidential-actions/2025/02/ensuring-lawful-governance-and-implementing-the-presidents-department-of-government-efficiency-regulatory-initiative/>.

¹⁸³ *In re Advanced Methods to Target & Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, Seventh Report and Order, FCC 23-37, ¶ 53 (May 18, 2023), <https://docs.fcc.gov/public/attachments/FCC-23-37A1.pdf>.

their business and the adverse effect on legitimate customers' experience, while leaving industry with the knowledge that a multi-million dollar enforcement action may be on the way should one single bad actor briefly elude those measures. That would be bad enough if bad actors could never adapt, but they do and are constantly trying to find new ways to circumvent providers' Effective Measures. This frustrating game of whack-a-mole makes strict liability an untenable and poorly conceived standard.

- iii The NAL's allusions to other potential measures that "may contribute" to meeting the Effective Measures rule show the Commission has not determined what is required of industry.

91. The Telnix NAL argues that apparent inconsistencies in the information provided to Telnix by MarioCop should have caused Telnix to (i) block the accounts or (ii) conduct further due diligence before allowing the accounts to place calls. We will review each alleged inconsistency in turn:

- IP address. There are numerous reasons why an IP address may be different from a caller's business address. Most obviously, the caller (i) may have outsourced calls to a customer support center or marketing center in a foreign jurisdiction, (ii) may be traveling, or (iii) may work for a company with multiple offices.
- Hotel address. Tens of thousands of people are hotel permanent residents or have long-term housing at extended stay hotels. It is not uncommon for an individual, a small business, or a sole proprietorship to use such a hotel address as a corporate address. In this case, Telnix contacted the hotel in question and confirmed that they offer extended stay options.
- Phone numbers. Telnix did not require a phone number during account creation (Telnix does now). The reason was simple: providing a phone number does not help with fraud detection. It is easy to circumvent two-factor authentication or purchase a burner phone, making this a near-pointless exercise in optics over substance.
- New email address. The Commission itself even acknowledged that there are reasonable reasons for possessing an email address like those provided by MarioCop.

92. Additionally, though the following language specifically applies to a provider's obligation to "effectively mitigate" illegal traffic under 47 C.F.R. § 64.1200(k)(4), it was adopted in the same docket as the "affirmative, effective measures" rule and is relevant to show the Commission's intentions when it promulgated these two interwoven requirements. The Commission stated:

"We decline to mandate specific metrics to make this determination, but expect that they will generally involve a significant reduction in the traffic stemming from a particular illegal calling campaign or regarding calls from the particular upstream

voice service provider[.] For example, if complaints clearly identify the specific campaign, a 50% reduction in complaints regarding that campaign may be sufficient to constitute effective mitigation, as that would likely represent a significant decrease in consumers receiving these calls . . . We expect that, where complaint reduction is judged relative to the entire call stream, the reduction may be smaller while still representing a significant decrease.”¹⁸⁴

93. As with the Effective Measures rule, the Commission also noted that it “do[es] not expect perfection in mitigation, nor do the rules we adopt require an intermediate or terminating voice service provider to block all calls from a particular source.”¹⁸⁵ Therefore, these similar rules are consistent in interpretation: the Commission requires reduction in unlawful traffic enforced by reasonable analytics and ex ante measures, not perfection.

94. Lastly, the Telnix NAL does not even clearly state what the alleged violations were for. Is the alleged violation that Telnix fails to maintain Effective Measures? The Commission stated that it “could likely find that Telnix apparently violated [the] rules with regards to every customer it onboarded using the same process as it did for the MarioCop Accounts.”¹⁸⁶ Does that mean even if Telnix can affirmatively identify every other customer, the mere act of onboarding each customer is a discrete Effective Measures violation? Is the Commission presuming evidence not in the record that every other customer was not identified and relying on that presumption in issuing the proposed fine? Since the Commission (erroneously) counts each call as a violation of the rules, the Commission appears to be saying that a provider could be fined for millions of lawful calls placed by customers it can identify on the theory that a single unknown customer taints the provider’s entire network. There is not a single provider that can accurately identify every single one of its customers—one only need look at the millions of prepaid SIM subscribers nationwide of numerous telecom providers. Furthermore, if violations accrue for every customer onboarded “using the same process,” then when would the violations end? After the next update to the provider’s Effective Measures (which happens constantly)? After a few new features are added? When there is a material alteration to the provider’s entire Effective Measures program?

95. Or is the alleged violation because Telnix did not know these specific customers? The Telnix NAL states: “Our rules require Telnix to know its customers. Yet it did not know . . . MarioCop[.]”¹⁸⁷ But, as noted elsewhere, the Effective Measures rule and the Commission’s own statements show that the Commission does not intend that a provider be able to infallibly identify every customer—only that its Effective Measures be “effective” in the more general, subjective sense. The Commission’s interpretation also doesn’t square with the Telnix NAL’s statement that Telnix could be liable for all customers it onboarded or even the Telnix NAL’s assertion that “Telnix had no effective KYC measures in place,”¹⁸⁸ which implies that the violation is not limited

¹⁸⁴ *In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, Third Report and Order, FCC 20-96, ¶42, n.100 (July 16, 2020), <https://docs.fcc.gov/public/attachments/FCC-20-96A1.pdf>.

¹⁸⁵ *In re Advanced Methods to Target & Eliminate Unlawful Robocalls*, 35 F.C.C. Rcd. 15221, 15232 (2020).

¹⁸⁶ Telnix NAL at ¶ 16.

¹⁸⁷ *Id.* at ¶ 16.

¹⁸⁸ *Id.* at ¶ 25.

to knowing any given customer but is, instead, an analysis of a provider's Effective Measures system as a whole.

96. Or is the alleged violation because Telnyx inadvertently allowed apparently illegal calls onto its network? The Commission calculated the forfeiture amount based on the number of calls placed by MarioCop, but if the call is the violation, then would there be any Effective Measures violations (and any penalty) if a provider allowed millions of unknown customers onto its network but none ever placed a call? The Commission never explained in the Telnyx NAL why a per-call penalty is appropriate for an alleged Effective Measures violation (financial regulators don't use a per transaction penalty for banks' alleged KYC violations). As noted in Section I, *supra*, the Commission's theory also appears to entirely ignore the Draft Eighth Report and Order issued just five months before the NAL that proposed an entirely different (and more industry-friendly) structure for both violations and penalties. Yet, even those more lenient proposals faced substantial industry opposition and were removed from the Updated Draft Eighth Report and Order.

97. From these examples, it is apparent that the Commission does not know and cannot articulate what clearly constitutes an Effective Measures violation or how the number of violations should be calculated. If the Commission does not know what constitutes an Effective Measures violation, then how can industry?

iv Telnyx's measures met or exceeded industry standards.

98. Telnyx, like other voice service providers, submitted its robocall mitigation plan to the Commission's Robocall Mitigation Database (RMD). These plans are publicly-available and provide a helpful approximation of other providers' robocall mitigation plans and, specifically, the Effective Measures that they employ. As noted previously, Telnyx was not one of the over 2,400 entities with deficient robocall mitigation plans listed in the RMD Cure Order. In fact, Telnyx's Effective Measures stand out as going above and beyond the industry consensus, as evidenced by a survey of the regulatory filings of Telnyx's competitors and USTelecom members.¹⁸⁹ At bare minimum, there is no cognizable argument that Telnyx's measures were inferior to those of its competitors or USTelecom members on the whole.

99. On February 27, 2020, then-Chief of the Wireline Competition Bureau, Kris Monteith, sent a letter to Telnyx and the rest of NANC's CATA Working Group thanking CATA for the "excellent work" and noting Chairman Pai's praise that "the prior NANC recommendations regarding call authentication represented a substantial step forward in ensuring that calls can be authenticated and verified."¹⁹⁰ Chief Monteith then directed CATA with recommending "best practices that providers of voice service may use as part of the implementation of effective call authentication frameworks,"¹⁹¹ and, specifically, whether "there [are] any other best practices

¹⁸⁹ See Robocall Mitigation Database Filing Comparison Chart (created Feb. 8, 2025) ("Exhibit G").

¹⁹⁰ See Letter from Kris Monteith, Chief, Wireline Competition Bureau, FCC, to Jennifer McKee, Chairperson, NANC (Feb. 27, 2020), <https://docs.fcc.gov/public/attachments/DOC-362809A1.pdf>.

¹⁹¹ *Id.* (quoting the TRACED Act).

voice providers can implement ‘to take steps to ensure the calling party is accurately identified?’”¹⁹²

100. Telnyx and CATA immediately got to work drafting best practices, culminating in the CATA Report that NANC sent to Chief Monteith on September 24, 2020. The CATA Report found that “[t]he general concept of subscriber vetting is embodied in the State Attorneys General/Service Provider Anti-Robocalling Principles,” specifically, Principle #3 (Analyze and Monitor Network Traffic), #4 (Investigate Suspicious Calls and Calling Patterns), and #5 (Confirm the Identity of Commercial Customers) (collectively, the “Principles”). The Principles are located in Appendix C of the CATA Report. Principle #5 recommends that providers obtain “physical business location, contact person(s), state or country of incorporation, federal tax ID, and the nature of the customer’s business.”¹⁹³ However, the CATA Report makes clear that these are merely “example[s]” and “may not apply to all VSP use cases or business models.”¹⁹⁴ The CATA Report then goes on to state, “Ultimately, VSPs should have the discretion to develop their own subscriber vetting program, which may include some combination of the practices summarized in this section, based on the types of subscribers they serve.”¹⁹⁵ Several USTelecom members explicitly state in their filings that their Effective Measures compliance programs are largely inspired by these Principles.¹⁹⁶

101. The *Fourth Report and Order*, released three months later, heavily emphasized the importance of allowing providers flexibility in selecting and implementing Effective Measures, which shows that the Commission ultimately adopted the CATA Report’s recommendations. Telnyx’s measures follow Principles ## 3 and 4 verbatim (which is why Telnyx was able to investigate and block MarioCop’s traffic so quickly). Consistent with the CATA Report’s recommendations, Telnyx’s measures combine portions of Principle #5 with other additional practices and procedures that Telnyx has found are more likely to stymie bad actors (e.g., substituting the federal tax ID suggestion with use of a third-party fraud decisioning platform). This is a reasonable approach consistent with the Effective Measures rule, the Effective Measures rule’s regulatory preamble, and the CATA Report.

102. Telnyx’s approach is demonstrably reasonable because it works.¹⁹⁷ Telnyx provides its unassigned numbers to YouMail for use as “honeypot” numbers to identify suspicious traffic.¹⁹⁸ If these numbers are called, it is highly likely that the caller is a bad actor since the numbers do not belong to any residential or cellular telephone number subscriber. By providing its honeypot numbers to YouMail, a third-party IT services provider, Telnyx can determine from which providers the majority of illegal calls originate. As it turns out, dozens of providers transmit more

¹⁹² *Id.*

¹⁹³ *See* CATA Report § 3.1.3.

¹⁹⁴ *Id.*

¹⁹⁵ *Id.*

¹⁹⁶ *See* Exhibit G.

¹⁹⁷ *See* Exhibit A ¶ 21.

¹⁹⁸ *See id.* ¶ 9.

illegal traffic than Telnix, including numerous USTelecom members and providers who require the same measures recommended in the Principles.¹⁹⁹ This demonstrates that no measures are perfect, and bad actors will find ways to originate illegal calls even if the Principles are followed verbatim. Telnix made the reasonable choice of using a third-party fraud decisioning platform, amongst other additional Effective Measures, and those Effective Measures have led to fewer illegal robocalls from Telnix's network than from the majority of Telnix's peers', which is the point of the Effective Measures rule.

V The Commission is violating *Jarkesy* and other constitutional obligations by bringing an in-house adjudication for monetary penalties without affording Telnix its constitutional right to a trial by jury.

103. The Telnix NAL similarly exposes the inherently unjust and unconstitutional system of the Commission's in-house adjudications for monetary penalties that, if allowed to stand, would violate America's fundamental principles of due process that President Trump's executive orders seek to protect.

104. President Trump has made making the federal government more accountable, fair and transparent a defining goal of his presidency. But the Commission's longstanding enforcement procedures are widely seen as in desperate need of reform. Thomas M. Johnson, Jr., who served as the Commission's General Counsel during the first term of President Trump, published a white paper highlighting the institutional flaws:

Not surprisingly, the agency almost always decides to initiate enforcement proceedings through the informal NAL route, which provides less protection to regulated parties and often with no meaningful ability to make its case to the Commission before the NAL is issued. As a result, [Enforcement Bureau] and FCC decisions concerning forfeitures are often insulated from judicial review. It also means fewer internal checks for [the Enforcement Bureau].²⁰⁰

105. The arbitrary discrepancies in fine amounts illustrate how the Commission's in-house adjudicatory system is broken. Robocalling enforcement actions can lead to monetary penalties ranging from just six cents per call to over \$4,000 per call for the exact same conduct. This leads to the conclusion that the Commission would rather shield the Enforcement Bureau from scrutiny than protect the constitutional rights of its targets.

106. None of this is new. Indeed, the first act of former Chairman Ajit Pai was to rein in a notoriously aggressive Obama-era Enforcement Bureau under its chief, Travis LeBlanc, who was widely viewed by industry as prone to issuing excessive fines. Chairman Pai revoked the Enforcement Bureau's independent authority to impose monetary penalties without a full Commission vote.

¹⁹⁹ See RRaptor Report (created on Feb. 23, 2025) (on file with Telnix and available to the Commission upon request).

²⁰⁰ Thomas M. Johnson, Jr., White Paper on FCC Enforcement Bureau Reform, at 5 (Jan. 29, 2024).

107. Unfortunately, Chairman Pai’s reform proved to be insufficient for what the Biden-era Commission had in mind. As noted above, the sole precedent cited in the Telnix NAL, the Lingo Telecom Consent Decree. But there is more to that story. The robocalls at issue in the Lingo Telecom Consent Decree followed an AI deepfake impersonating the president’s voice that was used in a robocall campaign during the New Hampshire Democrat primary. After the Biden Commission issued an NAL against a political consultant to a rival presidential candidate to Biden, the Commission next turned its sights on the telecom network that transmitted the deepfake robocalls, Lingo Telecom. According to press reports at the time, news of the AI deepfake instilled fear in Democrats that the president would be mocked through the use of AI deepfakes during the general election. Democrat pundits called on the Commission to protect the president from such AI-generated impersonations. Around that time, the Biden Commission also issued a proposed rule to mandate disclosure of the use of AI in political ads on television, which both Commissioners Carr and Simington opposed in part because they did not want political ad rules to change during an election.²⁰¹ The Biden FCC quickly came to the incumbent president’s rescue with the Lingo Telecom NAL, which was rightfully criticized by the same two commissioners.

108. The above demonstrates that, without significant constitutional safeguards, the Commission’s enforcement powers risk being wielded for political purposes, rather than neutral law-enforcement principles.

109. The Constitution imposes certain fundamental safeguard against such misuse of government power, including the Seventh Amendment’s guarantee of a right to trial by jury for most civil actions, constitutional separation of powers, and the Due Process Clause’s many guarantees—including the right to a neutral adjudicator.

110. The Commission should not proceed with this action because doing so would violate Telnix’s rights under the Seventh Amendment and the Fifth Amendment’s Due Process Clause. As Commissioner Simington recognized in his dissent from the NAL, the Supreme Court’s decision in *Jarkesy* precludes the Commission from extracting a civil penalty.²⁰² *Jarkesy* held that the SEC could not impose civil penalties through an administrative adjudication rather than by filing a complaint in federal court, affording the regulated person his “right to be tried by a jury of his peers before a neutral adjudicator.”²⁰³ Justice Sotomayor, in dissent, observed that the ruling would effect a sea change in the operation of the administrative agencies “that can impose civil penalties in administrative proceedings,” including the “Federal Communications Commission.”²⁰⁴ Exactly right. As Thomas M. Johnson Jr. concluded in his white paper on the enforcement bureau, “[a]s currently conducted, those proceedings are difficult to square with the

²⁰¹ Disclosure and Transparency of Artificial Intelligence-Generated Content in Political Advertisements, 89 Fed. Reg. 63381 (Aug. 5, 2024).

²⁰² See *SEC v. Jarkesy*, 603 U.S. 109, 140 (2024).

²⁰³ *Id.*

²⁰⁴ *Id.* at 200 (Sotomayor, J., dissenting).

Constitution, under which an Article III court and jury must be the adjudicator of a dispute involving private rights.”²⁰⁵

111. Of particular note are three obvious parallels between this case and *Jarkesy*:

Civil Penalty. The remedy here is identical to *Jarkesy*: a “civil penalty” imposed by the agency for an alleged violation of its rules. As such, “the remedy is all but dispositive” on the question of the unconstitutionality of the in-house adjudication.²⁰⁶

Intended to Punish. As in *Jarkesy*, the Commission’s order is also intended to “punish and deter, not to compensate” private victims.²⁰⁷ The Commission is not only “not obligated to return any money to victims,”²⁰⁸ but it definitively cannot do so because its forfeitures “shall be payable to the Treasury.”²⁰⁹ This makes the civil penalty “a type of remedy at common law that could only be enforced in courts of law,”²¹⁰ which the Court noted “effectively decides that this suit implicates the Seventh Amendment right.”²¹¹

Common Law Analogue: The Commission especially cannot regulate matters “in house” where its regulatory cause of action borrows from a “common law analogue.”²¹² The Commission’s actions seek liability for regulatory violations with “common-law private-right analogues,”²¹³ including, but not limited to, common law private nuisance, an action in debt, negligence, or unjust and unreasonable practices.²¹⁴ The claims at issue need not be “identical” to their common law analogue.²¹⁵ As noted above, a civil penalty is “all but dispositive” that a claim is legal in nature and, therefore, the Seventh Amendment is implicated.²¹⁶

²⁰⁵ Johnson, at 17.

²⁰⁶ *Jarkesy*, 603 U.S. at 123.

²⁰⁷ *Id.* at 125.

²⁰⁸ *Id.* at 124.

²⁰⁹ 47 U.S.C. § 504(a).

²¹⁰ 603 U.S. at 124.

²¹¹ *Id.* at 125.

²¹² *Id.* at 126.

²¹³ Johnson, at 17.

²¹⁴ See *Tull v. United States*, 481 U.S. 412, 418-19 (1987); Peter Karanjia, *The FCC’s enforcement process needs legislative reform following SEC v. Jarkesy*, at 11 (July 2024), <https://www.dlapiper.com/-/media/project/dlapiper-tenant/dlapiper/pdf/sec-v-jarkesy-white-paper.pdf?rev=-1>.

²¹⁵ 603 U.S. at 126.

²¹⁶ *Id.* at 123.

112. The above is not an exhaustive list of the similarities to *Jarkesy*, as the Commission’s choice to proceed with an “in house” adjudication raises several other constitutional flaws addressed by *Jarkesy*.²¹⁷ For instance, as discussed above, because the Commission itself—as well as its employees and their families—are listed in the NAL as victims of MarioCop’s unlawful calls, Telnix would have the right in a trial to seek recusal of any judge, prosecutor or member of the jury with an interest in the case (including as a victim). An in-house adjudication not only raises serious Seventh Amendment concerns but also fundamental concerns about Telnix’s due process right to advance reasonable defenses, engage in discovery, and have its case decided by a neutral adjudicator.

113. The Commission’s actions here also unlawfully violate constitutional separation of powers by combining “prosecutorial and adjudicatory functions within a single agency, the Commission’s enforcement regime” only multiplies the issues with this proceeding, especially considering that this is a special case in which the Commission finds itself the investigator and judge, as well as witness and victim.²¹⁸

114. The Commission has historically relied on *Atlas Roofing Co. v. Occupational Safety and Health Review Commission*, 430 U.S. 442 (1977), to justify its enforcement actions.²¹⁹ In *Atlas Roofing Co.*, the Court determined “that the adjudication of congressionally created public rights may be assigned to administrative agencies.”²²⁰ But *Jarkesy* expressly rejected the SEC’s expansive interpretation of public rights. As Peter Karanjia notes in his white paper on the subject, *Atlas Roofing Co.* is “a case of dubious vitality in the wake of *Jarkesy*.”²²¹ According to Justice Gorsuch in his concurring opinion in *Jarkesy*, “public rights are a narrow class defined and limited by history. As the Court explains, that class has traditionally included the collection of revenue, customs enforcement, immigration, and the grant of public benefits. . . . [O]utside of those limited areas, we have no license to deprive the American people of their constitutional right to an independent judge, to a jury of their peers, or to the procedural protections.”²²² This narrowing of public rights means most Commission actions, including this one, present claims that are legal in nature that must be litigated in an Article III court. Ultimately, concluded Karanjia, “the FCC’s Enforcement Bureau will not be able to continue with ‘business as usual.’”²²³

115. The Telnix NAL’s penal sanctions are also suspect on nondelegation grounds. The NAL stated that Telnix is a licensee because it made a filing in the RMD,²²⁴ and the Commission has “discretion” to pursue either an NAL or Notice of Opportunity for Hearing (NOH) as

²¹⁷ 603 U.S. at 117.

²¹⁸ Johnson, at 21; *see also Withrow v. Larkin*, 421 U.S. 35, 58.

²¹⁹ Karanjia, at 7.

²²⁰ *Atlas Roofing Co., Inc. v. Occupational Safety & Health Rev. Comm’n*, 430 U.S. 442, 456 (1977).

²²¹ Karanjia, at 9.

²²² 603 U.S. at 152-53 (Gorsuch, J., concurring).

²²³ Karanjia, at 14.

²²⁴ Telnix NAL at ¶ 18.

“[a]lternative procedures.”²²⁵ But the power to pursue multiple enforcement avenues with disparate rights for the enforcement target is “‘legislative’ in nature because it has ‘the purpose and effect of altering the legal rights, duties and relations of persons . . . outside the legislative branch.’”²²⁶ This legislative functioning raises nondelegation issues ripe for challenge.

116. Lastly, as relevant here, recent cases have held that challenges to the constitutionality of an agency adjudication can be brought before a final order where they challenge the “structure” or “procedures” of an agency.²²⁷ This is just such a case, since the in-house adjudicatory process employed by the Commission in this matter raises fundamental questions concerning the Commission’s enforcement-related structure and procedures.

VI Even assuming *arguendo* there was a violation, there is no factual basis for the allegation that Telnix engaged in willful or repeated violations of the Commission’s rules.

117. To justify its unprecedented and excessive proposed forfeiture, the Commission was required to conclude that Telnix’s alleged violation was “willful or repeated.” The Communications Act authorizes the Commission to levy forfeitures against regulated entities only in specific circumstances—not every instance of noncompliance or even a run-of-the-mill violation of the rules carries with it a forfeiture penalty. As relevant here, the NAL asserts its forfeiture authority under 47 U.S.C. § 503(b)(1)(B), which authorizes the Commission to impose a forfeiture penalty on any entity “who is determined by the Commission” to have “willfully or repeatedly failed to comply with any of the provisions of this chapter or of any rule, regulation, or order issued by the Commission.”

118. The NAL fails to offer any reasoned analysis, discussion or explanation for its determination that the alleged violation met this test: “Telnix apparently willfully and repeatedly violated section 64.1200(n)(4) of the Commission’s rules by failing to know its customers.”²²⁸ As discussed more below, any purported violation by Telnix (itself a wrong conclusion, *see supra*) could be neither willful nor repeated. But the NAL is deficient on this fundamental threshold issue: any agency order, no matter the applicable level of deference, must be “reasoned if it is to survive arbitrary and capricious review.”²²⁹ “That means the agency must adequately explain the facts . . . it relied on and its factual explanation must have some basis in the record.”²³⁰ The Commission’s

²²⁵ See 47 U.S.C. § 503(b).

²²⁶ Johnson, at 19-20 (citing *INS v. Chadha*, 462 U.S. 919, 952 (1983)); see also *Jarkesy v. Securities & Exch. Comm’n*, 34 F.4th 446, 451-465 (5th Cir. 2022).

²²⁷ See *Axon Enterprises, Inc. v. Fed. Trade Commission*, 598 U.S. 175, 180 (2023).

²²⁸ Telnix NAL at ¶ 17.

²²⁹ *Coinbase, Inc. v. Sec. & Exch. Comm’n*, 126 F.4th 175, 187 (3d Cir. 2025) (quoting *Env’t Health Tr. v. FCC*, 9 F.4th 893, 903 (D.C. Cir. 2021)).

²³⁰ *Id.* (citations omitted); see also *In re Sang Su Lee*, 277 F.3d 1338, 1344 (Fed. Cir. 2002) (in making a determination, an agency “must not only assure that the requisite findings are made, based on evidence of record, but must also explain the reasoning by which the findings are deemed to support the agency’s conclusion”).

failure to provide any explanation or analysis whatsoever connecting the facts of the case to its conclusion of willful and repeated violations is deficient and would not survive judicial scrutiny.

119. The Commission’s conclusion is also wrong on the merits. As recognized by the Commission and the courts, the definitions of “willful” and “repeated” in Section 312(f) of the Act apply to those terms as they are used in Section 503(b).²³¹ Thus, “willful” means “the conscious and deliberate commission or omission of such act, irrespective of any intent to violate any provision of this chapter or any rule or regulation of the Commission.”²³² Repeated “means the commission or omission of such act more than once or, if such commission or omission is continuous, for more than one day.”²³³

120. No willfulness. No reasonable finder of fact could conclude that Telnyx willfully violated the Effective Measures rule. As discussed above in detail in Section IV, *supra*, Telnyx has in place robust policies and robocall and fraud prevention measures, including extensive Effective Measures, which it refines and improves on a regular basis. Indeed, Telnyx is an industry leader in robocalling prevention and mitigation efforts, and has—until the issuance of the misguided NAL—maintained excellent standing with the FCC. Telnyx is also an official partner of the very consortium selected by the FCC to monitor robocalling and enforce industry compliance with the TRACED Act, the Industry Traceback Group. Indeed, although the NAL states that the Enforcement Bureau “obtained details pertaining to eight calls that reached Commission staff and worked with the [ITG] to use this information to trace the source of the calls,”²³⁴ it was Telnyx that reported the calls within 24 hours—before the Commission conducted its own traceback. This fact alone clearly demonstrates that Telnyx’s actions were not “willful.”

121. Further undermining any suggestion of willfulness is the fact that Telnyx itself is harmed when bad actors use its network. Among other things, Telnyx is forced to expend resources conducting more tracebacks, responding to subpoenas (and this NAL), and the like, and risks suffering reputational harm and customers within the industry, and friction with the Commission. Telnyx has strong incentives to specifically *not* violate the Commission’s rules and regulations, particularly as it pertains to Effective Measures policies, and always acts in accordance with that goal.

122. Finally, contrary to existing precedent involving the imposition of forfeiture penalties for willful violations in other contexts, Telnyx (and the rest of the industry) has never been informed what a violation of Effective Measures is.²³⁵ That is because the Commission itself

²³¹ *United States v. Unipoint Techs., Inc.*, 159 F. Supp. 3d 262, 272 (D. Mass. 2016) (citing Daniel R. Hicks, 30 FCC Rcd. 8437, 8437 n.7 (2015)).

²³² 47 U.S.C. § 312(f)(1).

²³³ *Id.* § 312(f)(2).

²³⁴ Telnyx NAL at ¶ 6.

²³⁵ See, e.g., *United States v. Angeles*, No. CV-19-16117, 2021 WL 2451971, at *4 (D.N.J. June 16, 2021) (“Defendant operated the unlicensed radio station over the course of three years, despite the FCC issuing various notices to Defendant about his unlawful conduct.”); *United States v. Polynice*, No. 21-CV-24243, 2022 WL 860381, at *1–2 (S.D. Fla. Mar. 23, 2022) (finding willful and repeated violations radio broadcaster operated its broadcast at a strength

has expressly declined to formally define, through proper rulemaking channels, what the Effective Measures rule specifically requires, despite industry pleas to provide such clarification. Telnix is thus left completely guessing as to what “act” it has apparently “conscious[ly] and deliberate[ly] commi[tte]d or omi[tte]d” as it pertains to “knowing its customers.”²³⁶

123. Not repeated. The forfeiture penalty is also improper because Telnix’s alleged violations were not repeated. As noted, repeated “means the commission or omission of such act more than once or, if such commission or omission is continuous, for more than one day.”²³⁷

124. First, even if it could fairly be said that Telnix violated the Commission’s Effective Measures requirements at all (it cannot), any such violation could not fairly be said to have occurred “more than once.”²³⁸ True, the NAL identifies two *accounts* that placed fraudulent calls. But, as is clear from the NAL, the accounts belonged to the same, singular *customer*: MarioCop. Both were registered to the same MarioCop business domain and were created on the same day. Both had the same physical address—which, at least at the time that Telnix collected customer information at registration, suggests the two accounts originated from the same business customer. Payment for both MarioCop accounts was made together, again reasonably suggesting a single customer. And even the NAL itself speaks in terms of MarioCop accounts, not accounts held by Christian Mitchell and Henry Walker.²³⁹ In other words, the NAL accuses Telnix of failing to know its *customer*, MarioCop, not the individual “employees” of its customer MarioCop, Mitchell and Walker.²⁴⁰ At most, two accounts were created, making it potentially appropriate to assess two violations *at most* (assuming *arguendo* there was a lawful basis to do so). The Commission’s contrary choice to assess a violation for each attempted *call* placed by that single customer is contrary to the regulatory text and contrary to the facts.

125. Second, because the Commission (improperly) seeks to impose individual forfeiture penalties for every individual call made by MarioCop, the Commission treats the violation as continuing in nature, lasting as long as the unlawful calls were being made. But Telnix stopped the calls within 17 hours, less than one day. Accordingly, the purported Effective

exceeding that permitted without a license on at least ten occasions over four years, despite numerous verbal and written warnings and equipment seizures).

²³⁶ 47 U.S.C. § 312(f)(1); Telnix NAL at ¶ 17.

²³⁷ *Id.* § 312(f)(2).

²³⁸ *See id.*

²³⁹ *See generally* Telnix NAL.

²⁴⁰ *See* Telnix NAL at ¶ 17. And of course, should the Commission find that each account was an individual customer subjecting Telnix to Effective Measures requirements, there would be, at very most, only two violations—one for each account—not 1,797 violations, which is what the Commission based its proposed forfeiture amount on. The use of the number of calls placed as a basis to calculate a forfeiture for an Effective Measures violation is arbitrary, capricious, and irrational for the reasons discussed in Section VII.

Measures violation (if any) cannot be deemed “continuous.”²⁴¹ As a matter of law, then, it cannot be considered “repeated.”

VII The Monetary Penalty Suggested by the Telnyx NAL Is Arbitrary, Capricious, and an Abuse of Discretion.

126. The Commission’s calculation of a monetary penalty for the alleged violation of the Effective Measures rule would be arbitrary and capricious if adopted. Under the APA, an agency action that is “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law” is to be set aside by a reviewing court.²⁴² An agency must rely on substantial evidence in its administrative record to support its findings, and there must be a “rational connection between the facts found and the choices made.”²⁴³ An agency’s findings are not supported by substantial evidence if there exists probative circumstantial evidence in the administrative record that the agency did not credit.²⁴⁴

127. The Commission, in deciding to propose a monetary penalty of \$4,492,500 has acted arbitrarily and capriciously because: (1) there is no rational connection between the number of illegal calls attempted by MarioCop and an alleged Effective Measures violation; and, (2) there is no rational connection between the alleged Effective Measures violation in Section 64.1200(n)(4) and the call blocking rule in Section 64.6305(g)(1).

- a There is no rational connection between the number of illegal calls attempted by MarioCop and an alleged Effective Measures violation.

128. The Commission’s proposed monetary penalty per call committed by MarioCop is not rationally connected to Telnyx’s alleged Effective Measures violation. The proposed penalty: (A) is wildly disproportionate to other volume-based forfeiture orders by the Commissions; and (B) is not connected to the alleged Effective Measures violation but instead attempts to impose a penalty on Telnyx for MarioCop’s violation of the Telephone Consumer Protection Act (“TCPA”).

- i The proposed penalty is disproportionate to other volume-based forfeiture orders by the Commission.

129. The Commission proposed a monetary penalty of \$4,492,500 for MarioCop’s 1,797 attempted calls at a rate of \$2,500 per attempted call.²⁴⁵ However, MarioCop only completed 1,117 of those calls. The Commission has arbitrarily imposed a per call penalty that includes 697

²⁴¹ See 47 U.S.C. § 312(f)(2). Penalties for continuing violations must be capped at \$2,449,575 for common carriers, 47 CFR 1.80(b)(2), though, as noted above, Telnyx’s one-way VoIP service is not a Title II service and calculating penalties on the basis of the common carrier maximum is antithetical to the Draft Eighth Report and Order.

²⁴² 5 U.S.C. § 706(2)(A).

²⁴³ See *Safe Extensions, Inc. v. F.A.A.*, 509 F.3d 593, 604 (D.C. Cir. 2007); *Burlington Truck Lines, Inc. v. United States*, 371 U.S. 156, 168 (1962).

²⁴⁴ *Allentown Mack Sales & Serv., Inc. v. N.L.R.B.*, 522 U.S. 359, 371, (1998).

²⁴⁵ See Telnyx NAL, para. 23.

attempted calls that were never completed. If calculated using the actual 1,117 completed calls, the penalty per call rises to a staggering \$4,021.93 per call.²⁴⁶ This is wildly disproportionate to past forfeiture orders based on the volume of illegal calls.²⁴⁷

130. As Thomas M. Johnson, Jr., notes, the Commission has a longstanding practice of issuing “unpredictable penalty calculations.”²⁴⁸ To illustrate this point, Telnix created Table 2, below, to show the vast and arbitrary discrepancies between per-call penalties across TCD’s enforcement actions:²⁴⁹

Table 2: FCC Robocall Monetary Penalty Comparison

Order Short Name	Penalty	Total Calls	Penalty per Call
Abramovich	\$120,000,000*	96,758,223	\$ 1.24
Roesel	\$82,106,000	21,000,000	\$ 3.91
Moser	\$9,997,750*	47,610	\$ 209.99
Rising Eagle	\$225,000,000*	1,000,000,000	\$ 0.23
Rhodes	\$9,918,000*	4,959	\$ 2,000.00
Robbins (NAL)	\$45,000,000	514,467	\$ 87.47
Burkman	\$5,134,500	1,141	\$ 4,500.00
Sumco Panama	\$299,997,000*	5,000,000,000	\$ 0.06
Dorsher	\$116,156,250*	9,763,599	\$ 11.90
Kramer	\$6,000,000*	9,581	\$ 626.24
Lingo (NAL)	\$2,000,000		\$ 502.77
Lingo (CD)	\$1,000,000	3,978	\$ 251.38
Telnix	\$4,492,500	1,797 ²⁵⁰ 1,117	\$ 2,500.00 \$ 4,021.93

²⁴⁶ See Table 2.

²⁴⁷ See *id.*

²⁴⁸ Johnson, at 3.

²⁴⁹ Although the table contains both spoofing and non-spoofing penalties (with different base forfeiture amounts), we note that the penalty per call appears much more highly correlated with total calls and the content of calls. See Table 3, below. For example, Rhodes’ \$2,000 per call penalty is much more closely related to Telnix’s \$2,500 proposed per call penalty than it is to other spoofing actions such as Abramovich, Roesel, or Rising Eagle.

²⁵⁰ Although the NAL suggests a larger number of calls were placed, Telnix has identified 1,117 completed calls. The Commission’s calculation of 1,797 appears to reflect MarioCop’s attempted calls.

**Indicates penalty amount after upward adjustment for egregious conduct.*

131. Past orders have heavily discounted bad behavior to the tune of mere pennies per call for the largest unlawful calling campaigns. The most egregious example of the Commission’s subsidization of bad behavior is *Sumco Panama*, where the Commission calculated a penalty for over 5 billion illegal auto warranty scam calls at a mere \$0.06 per call.²⁵¹ Contrast this rate with the *Burkman* forfeiture order, which was penalized at a rate of \$4,500 per call for 1,141 calls attempted election interference calls that included with racial animus.²⁵² Even more troubling, the Commission arbitrarily asserts millions, if not billions, of illegal calls were placed in its past forfeiture orders but then only verifies a small subset of calls, often in the mere single-digit thousands.²⁵³ In *Rising Eagle*, the Commission only verified 150 thousand calls out of over 1 billion illegal calls (less than 0.015%).²⁵⁴ In *Sumco Panama*, the Commission only verified 33,333 calls out of over 5 billion illegal calls (less than 0.00007%).²⁵⁵ But the Commission disproportionately punishes parties that the Commission deems apparently liable for a small number of calls, like Telnyx, because their small volume makes it possible to review all of the calls. This speaks to how arbitrary the Commission’s penalties are: the more calls a party makes, the lower their per-call penalty will likely be. By picking the number of calls it wants to verify and then upwardly or downwardly adjusting its base forfeiture amount (by up to thousands of dollars per call), the Commission arbitrarily employs back of the napkin math to arrive at whatever monetary penalty it wants—with wildly varying per-call penalties.

132. Additionally, while volume-based penalties are supposed to be content-agnostic, this is clearly not the case when examining past forfeiture orders. Telnyx created Table 3, below, to show how content, in addition to call volume, invariably affects the final forfeiture amount. The only calls penalized in the thousands per call were based on racial animus.²⁵⁶ The only calls penalized in the hundreds per call were based on election interference.²⁵⁷ Callers penalized from a few dollars to a few cents per call were mere scam callers.

Table 3: FCC Robocall Monetary Penalty Comparison Chart by Content Type

²⁵¹ *See id.*

²⁵² *See id.*

²⁵³ *See e.g., Philip Roesel, dba Wilmington Insurance Quotes, and Best Insurance Contracts, Inc.*, Forfeiture Order, 33 FCC Rcd 9204 (14) at para. 57 (2018) (explicitly recognizing the Commission only verifying less than one percent of calls is a significant discount); *Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc.*, Forfeiture Order, 33 FCC Rcd 4663 (7) at para. 7 (2018); *In the Matter of Rising Eagle Capital Group LLC*, Forfeiture Order, 36 FCC Rcd 6225 (9) at para. 59 (2021); *In the Matter of Sumco Panama SA, Sumco Panama USA*, Forfeiture Order, 38 FCC Rcd 7235 (8) at para. 3 (2023); *but see In the Matter of John M. Burkman, Jacob Alexander Wohl, J.M. Burkman & Associates LLC*, Forfeiture Order, 38 FCC Rcd 5529 (6) at para. 38 (2023) (no reduction in amount verified for 1,141 calls);

²⁵⁴ *See Rising Eagle* ¶ 59.

²⁵⁵ *See Sumco Panama* ¶ 57.

²⁵⁶ *See* Table 3.

²⁵⁷ *See id.*

Order Short Name	Call Type	Penalty per Call
Abramovich	Travel/Vacation	\$ 1.24
Roesel	Insurance	\$ 3.91
Moser	Election Interference (Local)	\$ 209.99
Rising Eagle	Insurance	\$ 0.23
Rhodes	Racial Animus	\$ 2,000.00
Robbins (NAL)	Insurance	\$ 87.47
Burkman	Racial Animus / Election Interference (National)	\$ 4,500.00
Sumco Panama	Auto Warranty	\$ 0.06
Dorsher	Scam / TDoS	\$ 11.90
Kramer	Election Interference (National)	\$ 626.24
Lingo (NAL)		\$ 502.77
Lingo (CD)	Election Interference (National)	\$ 251.38
Telnyx	FCC & Family Targeted	\$ 2,500.00 \$ 4,021.93

133. As numerous courts have held, “A long line of precedent has established that an agency action is arbitrary when the agency offer[s] insufficient reasons for treating similar situations differently,”²⁵⁸ and “[w]here an agency applies different standards to similarly situated entities and fails to support this disparate treatment with a reasoned explanation and substantial evidence in the record, its action is arbitrary and capricious and cannot be upheld.”²⁵⁹

134. The Commission has a demonstrated pattern of arbitrarily picking forfeiture amounts and attempting to justify them after the fact. This should concern anyone who cares about fair and impartial regulatory action. As the Supreme Court warned in *Fox Television Stations*, “precision and guidance are necessary so that those enforcing the law do not act in an arbitrary or discriminatory way.”²⁶⁰ But the Commission has long used its arbitrary forfeiture calculations to discriminate by volume and content to arrive at whatever number it wants, making it practically

²⁵⁸ *Kort v. Burwell*, 209 F. Supp. 3d 98, 112 (D.D.C. 2016) (citing *Cnty. of Los Angeles v. Shalala*, 192 F.3d 1005, 1022 (D.C. Cir. 1999)).

²⁵⁹ *Kort v. Burwell*, 209 F. Supp. 3d 98, 112 (D.D.C. 2016) (citing *Loc. 777, Democratic Union Org. Comm., Seafarers Int’l Union of N. Am., AFL-CIO v. N. L. R. B.*, 603 F.2d 862, 872 (D.C. Cir. 1978)).

²⁶⁰ *F.C.C. v. Fox Television Stations, Inc.*, 567 U.S. 239, 253 (2012).

impossible for a party to have fair notice of the potential penalty associated with an alleged calling-related violation until they receive an NAL.

135. The Commission justifies these disparate outcomes by arguing that it is not feasible for it to review every call for larger campaigns, but it is feasible for smaller campaigns.²⁶¹ This justification is not rational. The Commission's policy has the illogical effect of encouraging more illegal calls and punishing fewer calls. It also gives cover to the Commission to engage in discriminatory enforcement actions since, no matter the number of calls, the Commission can simply review as many as it desires to achieve the forfeiture it desires based on factors it should not consider (like call content). For example, Telnyx, the Lingo Telecom NAL, Kramer, Burkman, and Rhodes all involve campaigns of fewer than 10,000 total calls, yet the per call forfeitures vary from about \$500-\$600 per call in Lingo Telecom and Kramer to over \$4,000 per completed call in Telnyx and Burkman. Even in high-volume campaigns such as Rising Eagle and Sumco Panama (both with over a billion calls) the Commission verified wildly different numbers of calls: 150,000 in the case of Rising Eagle and 33,333 in the case of Sumco Panama. This conduct is not lawful.

ii *The proposed penalty wrongly attempts to enforce the TCPA on Telnyx for MarioCop's illegal calls.*

136. By proposing a penalty for each illegal call committed by MarioCop, the Commission is wrongly attempting to enforce the TCPA's illegal call prohibitions onto Telnyx for its customer's actions. The Commission does not allege that Telnyx violated the TCPA. But by imposing a per-call monetary penalty for each call, the Commission would effectively hold Telnyx liable for MarioCop's apparent TCPA violations.

137. An Effective Measures violation cannot be rationally connected to the prospective harm of an unknown quantity of illegal calls that a customer may make. An unknown customer, once granted access to a provider's network, can place anywhere from 0 calls to billions. Therefore, the Commission's assertion that Telnyx be penalized on a per call basis does not seek redress for an alleged Effective Measures violation, but instead seeks to enforce the TCPA against Telnyx as a proxy for its untraced customer.

b *There is no rational connection between the alleged violation of Section 64.1200(n)(4) and the call blocking rule in Section 64.6305(g)(1).*

138. The Commission is altering its past interpretations of Section 64.1200(n)(4) by analogizing it to Section 64.6305(g)(1), a reinterpretation of the regulations that is arbitrary and capricious, and contrary to law. An agency's findings are not supported by substantial evidence, and thus arbitrary and capricious, if there exists probative circumstantial evidence in the administrative record that the agency did not credit.²⁶² An agency acts arbitrarily and capriciously

²⁶¹ *In re Gregory Robbins*, Notice of Apparent Liability for Forfeiture, FCC 22-16 ¶ 33 (Feb. 18, 2022), <https://docs.fcc.gov/public/attachments/FCC-22-16A1.pdf>.

²⁶² See *Ohio et. al., v. Environmental Protection Agency*, 603 U.S. 279 (2024) (agency decision must be reasonably explained, and the agency must offer an explanation for its action including a rational connection between the facts found and the choice made and cannot simply ignore an important aspect of the problem.)

when it articulates a standard and does not apply it, and instead decides on a standard that it did not announce.²⁶³ An agency's interpretation of a regulation must not create "unfair surprise" for regulated industry.²⁶⁴ Regulated parties should have a reasonable expectation of the agency's interpretation and should not be caught off guard by unexpected or retroactive changes in interpretation.

139. The Commission: A) did not rationally identify the call blocking rule in Section 64.6305(g)(1) as an analogous violation for the purposes of setting an appropriate base forfeiture for the alleged violation, and B) chose Section 64.6305(g)(1)'s higher penalty than the Commission's own proposed rulemaking constitutes unfair surprise.

- i *The Commission incorrectly analogizes Section 64.1200(n)(4) to Section 64.6305(g)(1).*

140. While the Commission may look to an analogous violation where a statute is silent as to a base forfeiture, Section 64.6305(g)(1) is not analogous to an alleged violation to implement "effective measures." Section 64.6305(g)(1) specifically bases compliance on intermediate voice providers "accept[ing] calls directly from a domestic voice service provider only if that voice service provider's filing appears in the Robocall Mitigation Database."²⁶⁵ Therefore, it is rational to infer that an intermediate provider violating Section 64.6305(g)(1) should be penalized for each call that is accepted from domestic voice service providers without an RMD filing. However, this does not track the language of the Effective Measures rule that states that service providers must take "affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic."²⁶⁶ The obligation in Section 64.6305(g)(1) is objective and requires specific conduct, whereas Section 64.1200(n)(4) expressly does not require any specific conduct. Therefore, the best reading of both regulations is that Section 64.6305(g)(1) is violated for each accepted call from a deficient service provider, while Section 64.1200(n)(4) is violated per customer who is not ascertainable and places illegal traffic.

- ii *Selecting Section 64.6305(g)(1) constitutes an unfair surprise which contradicts its articulated standards from its proposed rulemaking.*

141. Picking Section 64.6305(g)(1) to find a base forfeiture also constitutes unfair surprise. Here, the Commission arbitrarily picked Section 64.6305(g)(1) to apply a \$2500 base forfeiture on a per call basis as if the Commission had not, mere months before, circulated for

²⁶³ See *Allentown Mack*, 522 U.S. 359 at 371.

²⁶⁴ See *Christopher v. SmithKline Beecham Corp.*, 132 S. Ct. 2156, 2168 (2012); *Long Island Care at Home, Ltd. v. Coke*, 551 U.S. 158, 159 (2007) (finding "unfair surprise" unlikely after agency underwent notice-and-comment rulemaking to change its interpretation of regulation).

²⁶⁵ 47 C.F.R. § 64.6305(g)(1).

²⁶⁶ *Id.* § 64.1200(n)(4).

public consideration the Draft Eighth Report and Order.²⁶⁷ The Draft Eighth Report and Order would set the base forfeiture for “failure to prevent customers from originating illegal calls” at \$11,000.²⁶⁸ But, crucially, the draft order states that the number of violations is to be set on a “per-customer, rather than per-call, basis” and would be based on “the maximum forfeiture that our rules allow us to impose on non-common carriers,” (emphasis added). While originally intended to go to a vote at the September 2024 Open Meeting, industry argued persuasively that draft order was too strict. But in the Telnix NAL, the Commission confoundingly adopts the maximum forfeiture for common carriers of \$251,322 per violation and a per-call penalty that goes far beyond what the hotly-contested Draft Eighth Report and Order would have imposed.²⁶⁹ Such conduct is unfair surprise and a lack of transparency with Telnix and industry more broadly.

142. Most concerningly, the notice of proposed rulemaking prior to the Draft Eighth Report and Order stated: “We do not believe that this will interact with the forfeiture ... for failure to block.”²⁷⁰ Failure to block, however, is the exact forfeiture to which the Commission now chooses to analogize an alleged Effective Measures violation. The Commission, by proposing a forfeiture of \$2500 based on the call blocking rule creates an unfair surprise for regulated parties because there is no nexus between the proposed Effective Measures forfeiture and the Draft Eighth Report and Order on which one would reasonably rely on to be a source of agency interpretation—especially when the agency had previously denied a connection between the two. Shifting to a per call forfeiture when the Draft Eighth Report and Order contemplates per customer penalties is plainly unfair, arbitrary, and capricious. The Commission’s actions are tantamount to regulation by enforcement and seek to bypass the established channels for rulemaking that the Commission had previously begun.

VIII Relief Requested.

143. Telnix respectfully requests that, before commencing work on the final order, the Commission immediately rescind the NAL for the reasons set forth above, including that voting members were affected by the activity in question. To the extent that any actionable claim remains available to the Commission under applicable law and the Administration’s executive orders, Telnix requests that the Commission re-adjudicate this matter with a properly-constituted panel of Commissioners upon the recommendation of unconflicted enforcement staff. In no event, on this record, should the Commission authorize a forfeiture penalty.

²⁶⁷ Draft Eighth Report and Order, ¶¶ 31-32.

²⁶⁸ *Id.*

²⁶⁹ Telnix NAL at ¶¶ 20-28.

²⁷⁰ See *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, 38 FCC Rcd 5404 (6) at ¶ 102 (2023).

EXHIBIT LIST

EXHIBIT A	Declaration of David Casem
EXHIBIT B	Declaration of Tom Walker
EXHIBIT C	Telnyx Letter to the Enforcement Bureau
EXHIBIT D	Consumer Complaints on Telnyx's Effective Measures Practices
EXHIBIT E	Y Combinator Hacker News Complaint on Telnyx's Effective Measures Practices
EXHIBIT F	Robocalling Enforcement Action Table
EXHIBIT G	Comparison of Robocall Mitigation Database Filings

EXHIBIT A

DECLARATION OF DAVID CASEM

1. My name is David Casem. In 2009, I founded Telnyx LLC (“Telnyx”) and, since then, have served as its Chief Executive Officer. I maintain residence in Austin, Texas.

2. I make this Declaration based on personal knowledge except as otherwise indicated. The information in this Declaration and in the Notice of Apparent Liability (NAL) response (“NAL Response”) is true and accurate to the best of my knowledge, information, and belief.

3. **Telnyx Background.** Telnyx is a private Voice over Internet Protocol (VoIP) services company with its principal place of business in Austin, Texas. Telnyx offers a variety of voice and data services, including communications IoT, networking, and compute services. Telnyx allows customers to obtain phone numbers and dial tones and offers both one-way and two-way, programmable voice services over the internet through the Telnyx API.

4. Telnyx does not operate a dialing platform. Telnyx’s customers cannot upload a list of phone numbers and simply dial them (commonly known as autodialer robocalling).

5. Telnyx is an established leader amongst VoIP service providers with a demonstrated commitment to—and vested interest in—preventing unlawful traffic. Prior to receiving the NAL, Telnyx had been a Supporting Partner of the Industry Traceback Group (“ITG”) since March 2020, providing support and guidance to the sole consortium selected by the FCC to conduct call traceback efforts.

6. Telnyx is an active participant in the North American Numbering Council’s (NANC) Call Authentication Trust Anchor (CATA) Working Group, the Numbering Administration Oversight Working Group (NAOWG), and nearly 20 other industry organizations and working groups, which we have provided in detail in the NAL Response. Through these leadership roles, Telnyx contributes its expertise to the ongoing development of numbering

policies that enhance the security and integrity of the telecommunications ecosystem. The CATA Working Group focuses on the technical and policy aspects of call authentication, particularly in the fight against illegal calls. Meanwhile, the NAOWG oversees the operational aspects of numbering, addressing issues such as number use, reclamation, and resale to mitigate potential abuse, misuse, and disuse within the numbering system. In these capacities, Telnyx has often worked with the FCC and at the FCC's direction to publish reports on fraud and illegal call prevention. Telnyx has also been an active participant in Commission rulemakings for many years, offering in good faith its feedback on how the industry can work with the Commission to reduce illegal calling. Finally, Telnyx has routinely cooperated with the Commission in its traceback and related investigations for many years.

7. As a result of the NAL, the ITG “suspended” Telnyx as a Supporting Partner, I have received death threats, Telnyx has suffered reputational harm, and our business has experienced higher than usual customer attrition, which I attribute to the negative reputational damage caused by the allegations in the NAL.

8. **Telnyx’s “Effective Measures” Practices.** To comply with, and even significantly exceed, the Commission’s robocall mitigation rules, Telnyx timely completed STIR/SHAKEN implementation and has implemented robust measures to comply with the requirements of Section 64.1200(n)(4) of the FCC’s rules (“Effective Measures”). Telnyx regularly updates and adjusts its Effective Measures practices to stay ahead of the “whack-a-mole” game in which increasingly sophisticated bad actors rely on advances in technology and evolving tactics to evade the telecom industry’s evolving defensive and preemptive measures. In reality, many well-established Effective Measures practices are often ineffective in this intensely combative environment. For example, the NAL argues, without any citation to authority, that Telnyx should have asked

prospective customers for an additional number, however, we had previously determined two-factor authentication is easily overcome even by unsophisticated bad actors using readily available numbers from websites that allow users to receive 2FA codes at no cost. Even the FCC's suggested requirement of a tax identification (ID) number is effectively window dressing. First, a tax ID cannot be a mandatory requirement because many legitimate prospective customers do not have a tax ID (e.g., they are consumers), and any bad actor knows how to generate a false tax ID, such as by setting up a shell organization (just as they know how to generate false driver's licenses and passports or pay third parties for the same). In other words, the FCC can try to come up with any number of ideas to mitigate risk, but the sophisticated bad actors are constantly adapting and changing tactics. No measures are capable of perfection. And as the FCC knows, it declined to adopt specific measures because it did not want to give bad actors advance notice of voice providers' specific measures – it wanted providers to have flexibility in this whack-a-mole game with the bad guys.

9. In addition to industry best practices, Telnyx also relies on creative measures to defeat bad actors. For example, Telnyx deploys “honeypots” for YouMail using unassigned Telnyx numbers to monitor illegal calls and help identify the origins of the traffic. Telnyx is not directly reimbursed for the costs associated with receiving calls on these honeypots in this manner; it is a service to the industry and consumers.

10. Telnyx's Effective Measures practices are robust. In addition to its Terms of Service and Acceptable Use Policy, Telnyx (i) requires that customers register with a business email address, physical location address, and business name (if applicable); (ii) tracks all customers' IP addresses to prevent banned customers from re-registering; (iii) tracks all customers' payment methods, scanning all payments for potentially suspicious patterns, (iv) contracts with

Braintree, a third-party fraud monitoring service and subsidiary of PayPal, to continually monitor payment methods with built-in anti-fraud measures; and (v) employs an industry-recognized, agnostic, third-party fraud decisioning platform managed by Sift Science, Inc. (“Sift”).

11. Telnyx uses STIR/SHAKEN to record both the identity header details and verification outcomes of customers’ traffic by downstream providers for analysis and monitoring purposes. Telnyx subjects all Telnyx-originated traffic to continuous monitoring, including monitoring of all IP addresses associated with blocked accounts and accounts that share domain names with suspended accounts. Telnyx also employs internal tools to examine the traffic metrics of all customers on an ongoing basis to detect fraudulent activity instantaneously, including monitoring for (i) excessively short average call duration rates, (ii) suspicious answer seizure ratios (i.e., the percentage of successfully connected calls relative to the number of attempted calls), and (iii) a high number of simultaneous active calls from a single account. Accounts less than two months old that display any of these patterns are immediately blocked. Telnyx performs daily routine script executions to detect newly registered users whose Calling Line Identification (“CLI”) display names include potentially suspicious keywords.

12. Telnyx possesses strong call origination and number verification policies and procedures. Telnyx validates a customer’s origination number against a global Do Not Originate list to prevent misuse and checks origination numbers against Nomorobo, a third-party database of known fraudulent numbers that is also used by the FCC’s Enforcement Bureau, to block potential threats. For U.S. domestic outbound calls, Telnyx (i) verifies the existence of an appropriate Local Routing Number (LRN) and blocks calls with non-existent LRNs, and (ii) does not allow calls with invalid CLIs to exit the Telnyx network. Non-Telnyx numbers intending to originate traffic from the Telnyx network are required to undergo number verification to prevent

spoofing (i.e., the display of inaccurate caller ID information). Telnyx receives daily complaints from potential customers—and Telnyx loses substantial business to competitors—specifically because of how stringent Telnyx’s Effective Measures practices are. But losing potential legitimate customers is a necessary cost to ensure that Telnyx and other providers do not allow illegal traffic onto their networks.

13. Lastly, Telnyx onboards all customers as “Level 1” (i.e., limited access) account holders, which includes significant limitations on available calling functionalities and global outbound calling limits. To reach “Level 2” (i.e., full access) status, customers must undergo rigorous additional vetting and call pattern review. Unless stated otherwise, the due diligence described above applies to both Level 1 and Level 2 customers.

14. **How and Why This Happened.** Telnyx onboarded MarioCop consistent with its standard Effective Measures practices for Level 1 accounts, and MarioCop purchased Telnyx’s one-way VoIP service. The MarioCop’s accounts scored outside the threshold for blocking but still within the range where Telnyx will closely monitor a customer’s traffic. Indeed, that’s how Telnyx proceeded with MarioCop – its close monitoring allowed Telnyx to shut down MarioCop after a brief period and low number of suspicious calls. With regard to the MarioCop calls, all of the information contained in the NAL is based on information that Telnyx voluntarily provided to the FCC. The NAL is correct that approximately 1,700 attempted calls were placed by MarioCop. But contrary to the implication in the NAL, I can say with confidence that MarioCop intentionally targeted the FCC. MarioCop placed a plurality of its calls to FCC employees, and many more of the calls not directed to the FCC were sent to telecom policy-related government officials, including the NTIA, the Department of Defense, U.S. Department of Justice, and other telecom-policy and industry participants, along with certain family members of FCC employees. Of the

approximately 1,700 calls attempted, only approximately 1,100 were completed. In other words, while the NAL implies that only “eight” or “over a dozen” calls unintentionally reached the FCC as part of a larger scam campaign, it is obvious this was a highly targeted campaign at a closed universe of regulators and telecom industry participants, including former and current FCC chairs, commissioners, and their legal advisors, rather than consumers. Although this information was voluntarily provided to the Commission, the failure of the NAL to more fulsomely and accurately explain the intentionally targeted nature of the campaign caused the trade press to assume the opposite – that the Commission personnel must have been unintentional “collateral damage” of a broader campaign. Further, in light of how the content of the calls could never deceive the sophisticated recipients of the calls (i.e., anyone at the FCC would know there is no such “Fraud Prevention Team” and even if there were, no FCC task force would push robocalls that make threats and demand compensation). Thus, oddly, it appears the bad actor primarily sought to disrupt and sow chaos within the government. The curation of this closed FCC-related universe of recipients and the skill with which the bad actors defeated strong Effective Measures while covering their tracks speaks volumes of MarioCop’s high degree of sophistication. For example, the NAL states that the personal cell phone numbers of the Commission staff, their family members (or even the identities of their family members), and other policy and industry insiders are not generally public information. The bad actors either were able to collect this information or had insider knowledge of and access to this private information.

15. The fact that Commission personnel, family and others in the telecom policy and industry ecosystem were targeted begs the question: Why would a sophisticated actor utilize such obviously fake content? Presumably, someone sophisticated enough to gather and curate such a targeted list would not limit their actions to transmitting such obviously fake content – they would

have some other nefarious goal, such as phishing to interfere with the Commission's operations. The incremental effort to do something more malicious would have been (presumably) low. But instead, the bad actors stopped at transmitting content that was fake by design. This appears to make little sense.

16. My own educated hypothesis is that the Commission was not the intended victim. The intended victim was Telnyx, and the Commission was "used" to trigger an enforcement proceeding against Telnyx. In a sense, Telnyx was effectively "swatted" – these calls were designed to trigger a reaction by the Commission, and it worked. In light of the undisputed facts in the NAL (provided voluntarily by Telnyx), I cannot conceive of a more rational explanation.

17. Nevertheless, Telnyx continues to routinely add even more advanced Effective Measures practices. Telnyx implements these measures due to our commitment to ensuring the integrity of our services and being an industry leader; we were not instructed to do so by the FCC or any other government authority. In March 2024, Telnyx began collecting credit card information before allowing customers to create an account. Based on the credit card information plus other account information, Sift creates credit card risk profiles for each customer. If Sift indicates an account is high risk or a customer requests the ability to place a high volume of calls, then Telnyx will require that account to be further verified by Onfido, a photo-based digital identity platform. Onfido requires that such customers provide multiple-angle photographs for identity verification. In April, Telnyx restricted the use of PayPal as a payment method to only Level 2 accounts. In May, Telnyx began requiring that all new accounts provide government-issued ID (this had previously only applied to accounts seeking Level 2 status) and instituted heightened monitoring for a customer's first 72 hours on the network. Finally, in July, Telnyx began restricting the use of Bitcoin as a payment method to only Level 2 accounts. These steps are not specifically required

by the FCC, but Telnyx implemented them in the interest of furthering the goal of robocall mitigation. Our measures continue to evolve.

18. The FCC should also be cautious about the unintended consequences of bringing this action against a longstanding compliant and cooperative partner in the Commission's efforts to clamp down on unlawful calls solely due to apparent evidence of "imperfection." The FCC's charter is to serve the public interest. Working cooperatively with industry to mitigate the scourge of illegal calls serves the best interests of consumers and industry alike – the public interest. Yet if the FCC regulates by enforcement to rewrite the governing standard of the Effective Measures rule as "perfection", then I predict industry will proceed with great caution whenever the FCC knocks and seeks voluntary cooperation. Companies have an independent regulatory duty to act in the best interest of their shareholders, and if the FCC is going to regulate by enforcement to pursue a mandate of perfection that was not adopted with notice and comment, companies will have no choice to retract the open hand of cooperation and take a more defensive stand against such unfair government actions. Telnyx has a proud track record of voluntary cooperation and responsiveness (including in this matter) and participation in joint public-private organizations to combat bad actors. But the NAL's approach will send a chilling message to industry and undermine the public interest.

19. As discussed above, the Effective Measures practices described herein are far in excess of industry standards. Based on my two decades of experience in the industry, I am confident that Telnyx's Effective Measures practices match and often far exceed those of the vast majority of Telnyx's peer and competitor voice service providers, including many respected service provider members of USTelecom. Prior to our receipt of the NAL, the FCC had never

communicated to me—or, to my knowledge, anyone else at Telnyx—that it believed Telnyx’s Effective Measures practices to be non-compliant.

20. The Commission’s Effective Measures rules do not, and never should, require “perfection.” And the fact that a single bad actor defeated Telnyx’s Effective Measures is not evidence of a violation. If that were the case, then the standard would be perfection, which no voice service provider can possibly obtain. On February 7, 2024, Telnyx’s robocall mitigation analytics alerted Telnyx to a potential illegal calling campaign. Telnyx promptly investigated and blocked traffic from the call originators—MarioCop—within 17 hours. That is not slow – that’s very fast. Only approximately 1,100 calls were completed, which is a very low number relative to other FCC robocall enforcement proceedings.

21. Within two days of our letter declining the tolling agreement, Telnyx received the NAL, which was surprising because the NAL does not identify any actual noncompliance with the Effective Measures rule. Telnyx maintains that it has implemented industry-leading, fully compliant robocall mitigation measures, as evidenced by the fact that (a) Telnyx blocked approximately 49.5% of all attempted new customer signups, (b) only about 0.2% of Telnyx customers who used our service in 2024 were ever associated with a traceback, and (c) Telnyx swiftly mitigated the MarioCop traffic. If the FCC feels that Telnyx’s Effective Measures practices are deficient with its expectations, or it wants to elevate the standard to perfection, then the FCC should initiate a notice of proposed rulemaking and seek industry comment, not legislate through regulation by enforcement against an industry leader.

22. Unfortunately, because the NAL surprisingly moves the goalpost of what constitutes “Effective Measures,” the FCC is likely to both chill industry participation in illegal

call mitigation and chill the industry's appetite for new technologies and differentiated anti-fraud measures – the very things that the FCC should be acting to foster among industry participants.

I declare under penalty of perjury that the foregoing is true and correct. Executed on February 27, 2025.


Signature:  _____
David Casem
CEO, Telnyx LLC

EXHIBIT B

Declaration of Tom Walker

I, Tom Walker, have personal knowledge of the matters set forth below.

Background

1. I have worked as a telecommunications fraud manager, analyst, and investigator for the past twenty-two years. In that capacity, I managed fraud investigations at T-Mobile, USA for ten years, and, subsequently, AT&T for another ten years. By my best estimate, investigations in which I have led or supervised and participated have (i) resulted in more than 1,000 arrests, (ii) been cited before the Supreme Court, and (iii) been the subjects of numerous articles in the Federal Journal of Criminal Practice.
2. I am an original contributing founder of the Industry Traceback Group (ITG) and, in that capacity, helped draft the ITG's policies and procedures between 2016 and 2020. I personally recruited several hundred VoIP providers to voluntarily participate in traceback processes pursuant to 47 U.S.C. § 222(d)(2). I have also contributed to a wide variety of trade groups, including the Communications Fraud Control Association, the GSMA Fraud and Security Group, the i3Forum, the Global Solutions Council, and the Revenue Assurance Group, and am one of the founding contributors of Europol's Cyber-Telecom Working Group.
3. I have referred actionable evidence in more than 100 cases of illegal calling to various law enforcement agencies, resulting in more than seventy-five arrests in the United States, India, and the Dominican Republic. I have personally traced more than 2.5 million spoofed illegal calls, plus tens of millions of non-spoofed illegal calls.

Robocalls from "MarioCop"

4. On February 4, 2025, the Federal Communications Commission (FCC) issued a Notice of Apparent Liability (NAL) to Telnyx LLC ("Telnyx") for calls made by an entity holding itself out as "MarioCop" (the "Calls").¹ The NAL alleges that MarioCop sent prerecorded messages demanding money while claiming to be from a fictitious "Fraud Prevention Team" at the FCC. Shortly thereafter, Telnyx asked me to examine the Calls. I reviewed 1,029 Calls² made to 791 unique phone numbers between 5:59 PM and 9:04 PM ET on February 6, 2024.

Calls to FCC Staff

5. Based on my experience in conducting investigations that have been admitted into evidence in numerous court cases and relied upon by law enforcement, I leveraged the following public resources: Trestle, LinkedIn, GitHub, FastPeopleSearch, FastBackgroundCheck, Pipl Data, Whitepages.com, Cognism, and Justia. I have found these resources to be reliable and accurate in similar investigations. In this case, I confirmed that nearly half of the Calls were

¹ Telnyx NAL ¶ 1.

² The email address associated with the calls from this MarioCop account is christian@mariocop123.com.

completed to the personal wireless, home, or office numbers of FCC employees. With regard to the other approximate half, many of such Calls were made to persons who (i) had similar or identical names to FCC employees, (ii) were other government officials, particularly in the telecom-adjacent sector, or (iii) were persons who are privately employed in the telecom policy sector. Lastly, there were certain calls to individuals that did not appear to be employed by the FCC or other telecom-related organizations, but based on the NAL's statement that family members of FCC employees were called, it seems reasonably likely that at least some of these recipients were family members or former FCC employees.

6. After carefully reviewing the totality of the information gathered through my examination of the calls, the evidence clearly indicates that the intent of the Calls was not to defraud consumers but, rather, to call and harass as many FCC employees as possible, including senior leadership. Based on my findings, it is all but certain that this MarioCop account intended that all of its calls reach FCC employees, telecom-policy related institutions, and other government officials.
7. I determined that MarioCop targeted FCC leadership, including:
 - One call to then-Commissioner Brendan Carr.
 - One call to the current Chief of Staff to Chairman Carr.
 - Two calls to a Legal Advisor to then-Commissioner Carr.
 - Three calls to the former Chief of Staff to then-Commissioner Carr.
 - One call to Commissioner Nathan Simington.
 - Two calls to two different Legal Advisors to Commissioner Geoffrey Starks.
 - Four calls to the Chief of Staff to Commissioner Anna Gomez.
 - One call to a Policy Advisor to Commissioner Gomez.
 - Five calls to a Legal Advisor to Commissioner Gomez.
 - One call to a Senior Policy Advisor to former Chairwoman Jessica Rosenworcel.
 - Two calls to the Chief of Staff to former Chairwoman Rosenworcel.
 - Three calls to the Chief Legal Advisor to former Chairwoman Rosenworcel.
 - Four calls to three phone numbers associated with former Chairman Ajit Pai.
8. In total, I determined that MarioCop made Calls to at least 365 phone numbers associated with FCC offices, staff, and former staff. I also discovered calls to phone numbers associated with Congressional Offices, a U.S. District Court Judge, a U.S. Attorney's Office, two States Attorneys Generals Offices, the Universal Service Administrative Company, other government and law enforcement agencies, and numerous telecom policy-related trade associations and law firms.
9. Telnyx's business records indicate that it disconnected MarioCop at 6:20 AM ET on February 7, 2024. Telnyx's records also indicate that it received traceback requests from

other voice service providers ten hours later via the ITG between 4:04 PM and 7:37 PM. In many cases, the tracebacks were initiated for Calls made to individuals holding significantly more senior roles than those referenced in footnote 17 of the NAL, including:

- Traceback request 16810 for calls to a Legal Advisor to Commissioner Starks.
- Traceback request 16803 for calls to the Deputy Chief of the Enforcement Bureau.
- Traceback request 16804 for calls to a Deputy Division Chief of the Competition Policy Division.
- Traceback request 16806 for calls to the Acting Bureau Chief of the Consumer and Governmental Affairs Bureau.

10. Based on the totality of this information and the content of the calls described in the NAL, I concluded that MarioCop apparently did not intend to defraud FCC staff by calling them and impersonating a non-existent FCC department. Nor did MarioCop apparently defraud anyone, as none of the Calls lasted longer than two and one-half minutes.

I declare under penalty of perjury that the foregoing is true and correct. Executed on February 25, 2025.

Signature: 

EXHIBIT C



Perkins Coie LLP
700 13th Street, N.W.
Suite 800
Washington, D.C. 20005-3960

T. +1.202.654.6200
F. +1.202.654.6211
perkinscoie.com

January 30, 2025

VIA ELECTRONIC MAIL

Daniel Stepanicich
Deputy Division Chief
Telecommunications Consumers Division, Enforcement Bureau
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Marc S. Martin
MMartin@perkinscoie.com
D. +1.202.654.6351
F. +1.202.654.9113

cc: Patrick.Webre@fcc.gov
Kristi.thompson@fcc.gov
Jane.vanbenten@fcc.gov

Re: Case File No. EB-TCD-24-00037170

Thank you for the call last night to discuss the proposed tolling agreement with Telnyx LLC (“Telnyx”). As you know, Telnyx sent you a letter yesterday explaining that we needed more information from the Enforcement Bureau to inform whether we could agree to your request for a tolling agreement. You emailed our client, Telnyx, last night shortly after 5:00pm and requested a call immediately. Telnyx agreed and proceeded with the call that included the undersigned as its counsel at 6:30pm last night (the “Call”).

Statutes of limitations provide basic, statutory rights to Americans in a wide range of contexts, including statutes providing for civil penalties. The proposed tolling agreement asks Telnyx to waive its rights and extend the Communications Act’s one-year statute of limitations for a specified period. In the Call, we explained that we are entitled to certain basic information so that we can provide informed consent to the tolling agreement request. Specifically, we asked the following questions:

- Why is the tolling needed?
- Is Telnyx the target of an impending enforcement action?
- What specific rules did Telnyx allegedly violate, and how?
- What does Telnyx get in return for granting the FCC’s request?
- What happens if we do not agree? Are there any specific adverse enforcement measures contemplated?

We received very little information in response to these questions. Your response to why the tolling was needed was that “leadership” needed more time to decide how to proceed with our case. You declined to clarify what you meant by “leadership.” You declined to answer if Telnyx was a target of an investigation. You responded to our question about what violations you allege with a reference to the tolling agreement’s citation to 47 CFR § 64.1200(n)(4). But that cited rule vaguely requires “reasonable” know-your-customer (“KYC”) requirements without any more specificity. And you declined to clarify what Telnyx may have specifically done to allegedly violate this cited rule. You could not offer any benefit in return for agreeing to the tolling agreement nor address whether Telnyx may face retaliatory action if it declines the request. In fact, when we asked in summation, “So you are basically asking us to just trust you?” you responded “That’s right.” These responses do not provide us with sufficient information for informed consent.

We also discussed the precedent on which you relied in pursuing this potential action against Telnyx, which you confirmed to be the Lingo Telecom enforcement action in May of 2024. But Lingo Telecom is not precedent for this situation.

First, Lingo Telecom did not reach a final Notice of Forfeiture voted on by the full Commission. It was resolved by settlement and consent decree without a full Commission vote. As such, it is not appropriate precedent, especially now that President Trump’s Executive Order 13892 prohibits all federal agencies, including independent agencies, from engaging in “regulation by enforcement.”

In fact, the two Republican members of the Commission at the time, Brendan Carr (now Chairman) and Nathan Simington, both were highly critical of the [Lingo Telecom NAL](#) because it appeared to be a case of rulemaking by enforcement (emphases added):

(Then-)Commissioner Carr: “In this case, it is apparent that the person who orchestrated this robocall scheme violated the FCC’s rules. And I have voted to approve that Notice of Apparent Liability. With respect to the voice service provider that the caller used to originate the calls in question, the FCC alleges here that the provider failed to implement STIR/SHAKEN. The FCC’s argument is not that the provider took no steps to implement the STIR/SHAKEN framework. Rather, the NAL alleges that the steps the voice service provider took to implement the framework failed to apply the correction attestation level. Although these allegations will require careful review, **I will also be focused on ensuring that the FCC does not undertake “rulemaking through enforcement” by creating new, substantive obligations that go beyond the standards set forth in our existing rules. We need to be careful that we do not undermine reasonable reliance on prior FCC decisions and spring enforcement on parties seeking to comply in good faith.** With that said, NALs are not final decisions on the merits. I will keep an open mind as the FCC reviews the record in this proceeding.”

Commissioner Simington: “Lingo states in its defense that it relied on Life Corp.’s contractual statements about numbers and permissions in what the Enforcement Bureau notes was a one-page form with no diligence backing it up. This might not be the most sympathetic defense, but it isn’t an unreasonable one, because the FCC has never required a higher standard. This is why the FCC has to have recourse to vague statements like “reasonable KYC [know your customer] protocols,” and needs to make a novel finding that a “generic, blanket, check-the-box ‘agreement,’” is insufficient, in order to find liability. **All voice providers nationwide are surely taking note of the FCC’s actions today, but it’s not actually clear what their obligations now are. Must they immediately implement KYC and, if so, to what standard?** If their current client contracts are inadequate, must they require that all clients sign new ones and, if so, what should the new contracts say? If they fail to do so, ought they to expect to be fined \$1,000 per call? These are completely open questions because the FCC has never engaged in a rulemaking on this matter, delegating it instead to an industry group and to industry standards. The problem for our action today is that Lingo probably complied with industry standards. We might deplore the laxity of these standards, but Lingo might well respond that they were in line with actions that had been repeatedly blessed by the FCC. **And today, by using an enforcement mechanism to declare new standards (however vague,) we are engaged in a back-door rulemaking through enforcement.** I decline to say that the FCC can never do this, because some situations are so urgent or egregious that we have to have the option. But every time we do, the next step should be to start a rulemaking immediately, and the step after that should be to ask how we allowed the situation to devolve such that we needed to use what ought to be an emergency power. As such, I concur with the majority while noting that the FCC must immediately act to establish clear standards within which the industry can operate.”

As Telnyx stated in its letter to you yesterday, rulemaking by enforcement violates [Executive Order 13892](#), which was initially issued by President Trump in 2019, rescinded by President Biden, and reinstated last week by President Trump. It also prohibits Executive Branch agencies, including independent agencies, from engaging in “surprise” enforcement matters by calling on agencies to rely solely on published rules of general application and providing notice of the actions that will be considered violations of those rules. It appears the Enforcement Bureau is ignoring President Trump’s Executive Order 13892. Chairman Carr and Commissioner Simington’s criticisms of the Lingo Telecom NAL were remarkably prescient, not only as to Lingo Telecom’s final settlement, but also what appears to be happening in this case.

Further, we noted that we reasonably believed that Telnyx’s months of correspondence with the Enforcement Bureau during the Biden administration about certain callers on our network was in the spirit of cooperation, consistent with our mutual goal of stemming caller misconduct. As you know, Telnyx has long supported and cooperated with the FCC to mitigate unlawful caller conduct, including as a Supporting Partner of the Industry Traceback Group. Telnyx was surprised that, through its routine cooperation with the FCC, it suddenly became a target. This turning the tables on Telnyx undermines the public policy

of working with industry cooperatively. That is, an enforcement proceeding against a carrier with a stellar record of compliance and cooperation will cause the broader telecom industry to be on guard and reluctant to engage with the Commission voluntarily. This consequence would not serve the public interest.

Another reason for Telnyx's surprise was that, just last month, the Commission issued a list of allegedly non-compliant parties that did not include Telnyx. This gave us the reasonable impression that the Commission believes Telnyx's robocall mitigation measures are compliant. Specifically, on December 10, 2024, the FCC issued a list of 2,411 [carriers](#) that it asserted were noncompliant with the FCC's Robocall Mitigation Database filing requirements for their failure to properly certify compliance with STIR/SHAKEN implementation, describe their robocall mitigation plans, or provide other required information that the FCC uses to monitor compliance. Those carriers listed among the 2,411 would have to show cause why it should not be removed from the Robocall Mitigation Database. Carriers **NOT** listed apparently had their certifications accepted by the Commission as compliant. Telnyx was **NOT** listed. To change course now would be an unfair surprise in violation of Telnyx's due process rights, not to mention a violation of Executive Order 13892.

Finally, after Lingo Telecom, the Supreme Court found in *SEC v. Jarkesy* (2024) that adjudications by federal agencies that seek monetary penalties are unconstitutional. Any similar agency enforcement action against Telnyx would be contrary to *Jarkesy* and would not survive judicial review.

In short, due to the failure to respond to our reasonable questions about the need for the tolling agreement, and the admitted reliance on a suspect precedent, Telnyx must respectfully decline to agree to the proposed tolling agreement.

Respectfully,

A handwritten signature in black ink, appearing to read "Marc S. Martin". The signature is fluid and cursive, with the first name "Marc" being the most prominent.

Marc S. Martin
David W.T. Daniels
Brandon R. Thompson
Addison W. Bennett

EXHIBIT D



Ghazanfar Abbas

6 reviews  PK



Jan 31, 2025

Unable to signup

Unable to signup . They blocked my account immediately when I attempted to verify via email. And after that they said they are not accepting signup requests from pakistan. This is what, I wasted my hours on it

Date of experience: January 31, 2025



m.

1 review  CZ



Updated Dec 9, 2024

Scam

Scam. And I was stupid enough to fall for it even though I read the negative reviews here.

I created a business account for our company, ordered a phone number, verified my identity via Onfido and submitted all the verification documents they asked for. They charged us for the services and few hours later blocked our account during the verification process without any reason and without returning the money.

Edit: even if they may have blocked us by accident, deleting our account without any previous warning is a terrible approach. The consequences for our customers and our business would be huge if we implemented Telnyx as part of our processes. If this company is not scam (which I'm still not sure about), then it is definitely a product to avoid at all costs.

Date of experience: December 06, 2024

 Useful 1  Share



Reply from Telnyx

Dec 9, 2024

We actually have strict security measures to protect against scammers and spammers, a security measure you may have set off on accident. We typically automatically refund to the payment method on file but if you have not received it, please reach out to billing@telnyx.com!

PK**Peter Knappertbusch**5 reviews  GB

Oct 8, 2024

Telnyx BTC lost without warning

Telnyx accepts BTC payments but directly blocks the account without reason when you travel on holiday and login from another country. You loose everything!

Date of experience: October 09, 2024

 Useful  Share

**Reply from Telnyx**

Oct 9, 2024

Hi Peter,

Thank you for your feedback. We have strict security policies to ensure fraud is prevented on our network. If you feel your account has been suspended inaccurately, please feel free to give us a call at +18889809750 ext 992 and we will review this straight away.

Regarding your payment, we will always refund unused funds on your account if you no longer want to use it. Please send a request to billing@telnyx.com to start the process to initiate a refund at any time.

Thanks!



chris

12 reviews  GB



Mar 23, 2024

Asking me again to fill in a kyc form

Asking me again to fill in a kyc form, I have already done this once, This is what you can expect with Telnyx, go all round the houses for weeks to get back to square one. I already switched to Clicksend, and got my first sms sent within half a day including software development.

Date of experience: March 18, 2024

 Useful

 Share



Reply from Telnyx

Mar 25, 2024

Hi! Sorry for any inconvenience. We are dedicated to keeping spammers and scammers off of the platform so sometimes a legitimate use case can get caught in the net. It is easy to get your first message on Telnyx sent within minutes for most users so when Clicksend drops the ball we will be happy to support you again!



Joshua Nissenbaum

2 reviews AU



Dec 4, 2023

Really Poor Experience

Created an account and purchased some credits to implement the Messaging API. Account was blocked automatically by the system - no reason given. I used a credit card that matches my name, and I registered with my company email. So they've taken my money for credits, locked me out and won't reply over email.

Support has been of 0 assistance, and takes 24 hours to reply. Live Chat is unavailable, because I cannot login.

They are one of the cheapest providers - this is the reason why.

Date of experience: December 03, 2023

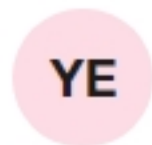
Useful Share



Reply from Telnyx

Dec 5, 2023

Hi Josh! Thanks for sharing! We want you to have a smooth experience! Your account has been unblocked now. Please let us know if there is anything else we can help with!



Yusuf Emre

5 reviews



GB



Feb 1, 2025

They simply don't delete your data, and they claim they do it.

I signed up their platform, and I got automatically blocked right after I click the submit button on the registration form. I have never used their platform, never had any interaction with them or anywhere related to them. My IP is a clean IP, my e-mail is a corporate e-mail that exist over 10 years, my e-mail server uses EV SSL. I can further add details, but no needed, because it's simply nothing on my end.

I reached out for this red flag immediately, and I did not like the idea of blocking people right at the registration form. This is a major red flag. You may get blocked without any cause if you are getting block right at your first interaction.



Hue Quang

1 review  US



Dec 17, 2024

Support from this company is a joke...

Support from this company is a joke !!!!! seems like answers from them are robot or AI created. It makes no real effort to solve an account blocking problem which triggered by their stupid KYC verification flow !!!

Date of experience: December 17, 2024



Sean F

11 reviews  US



Oct 5, 2024

Vague credit card stuff

Vague credit card stuff, suspended for no reason, if I had been with them more than I was, my company would have suffered greatly. How do you get suspended for not breaking rules?

I posted a blog post about it.


Horrifying.

The fake reviews are even worse.

[why-you-should-avoid-telnyx-unreliable-service-and-serious-regulatory-issues/](#)

:/

Date of experience: October 04, 2024

 Useful  Share



Reply from Telnyx

Oct 7, 2024

We do have strict security measures. If you feel you have been suspended for no reason please feel free to give us a call at +18889809750 ext 992 for us to review it.



wij ay

1 review US



Oct 3, 2024

Beware: Telnx Blocks Accounts Without Reason and Keeps Your Funds!

I am extremely disappointed with Telnx and want to share my experience to warn others. I deposited \$100 in Bitcoin into my account, which was then blocked without any clear explanation. Despite sending numerous emails asking for clarification, I was given vague responses and told that my account was permanently blocked due to "internal policies," without any further details.

Not only did Telnx refuse to provide a reason for the block, but they also denied the refund of the Bitcoin I deposited. To make matters worse, I verified my account by providing my documents and a video selfie as requested. Now, not only have they kept my funds, but they also have my personal documents, which I find extremely concerning.

Their actions can only be described as a scam. They have essentially stolen my money and my documents, with no transparency or customer support.

If you're considering using Telnx, beware—they can block your account without explanation, keep your funds, and take your personal information. I wouldn't want anyone else to go through what I have experienced. Avoid this company if you value your money and personal security.

Date of experience: October 03, 2024

Useful Share



Reply from Telnx

Oct 3, 2024

Hi! We do have strict security policies be we will always refund unused funds on your account. Please send a request to billing@telnx.com to initiate a refund. Thanks!



David

1 review

📍 US



Aug 6, 2024

Don't use Telnyx, find someone else

I've been using Telnyx for the past few months and it's been okay. When I created my account, I was told that I needed to send my identification to them, like many other providers do. That's fine, I do it and it happens. Then they move to a "new system" where I have to give my identification to them again. The only reason why I'm logging in is to pay my bill before I lose my services and to fix an issue, because my phone service which I PAID telnyx for isn't working. Annoyingly, I did it, even though they did who knows what with my ID before. Then they say my identification card isn't accepted. It's a Georgia (USA) Driver's License. I call their 24/7 support and they tell me that I need to do it again or E-mail their support, which a lot of times can take hours to get something resolved. I'm done with Telnyx at this point and I ask the agent can I port my number to another company. She says yes and that I need to sign-in to the portal to do it. I can't even sign in to the portal to use the products I am paying for. This is just shameful

Date of experience: August 06, 2024



Paul

3 reviews



GB



Jun 14, 2024

onboarding not working

guys you need to sort out the onboarding process - I am a new customer who has added a card to join (Paypal) and now you have disabled that and just left me with Bitcoin as a payment method?

Email 2 (2mins later)

Our review of your account details by our team found that your account doesn't meet our credit card safety and chargeback protection guidelines. As a result, credit cards and PayPal are no longer eligible payment methods for your account. You are welcome to attempt the remaining payment methods.

Email 1:

On review of your account details, your credit card has been accepted. You may proceed to the Telnyx Mission Control Portal to make a payment.

Date of experience: June 13, 2024



Arcwell Hernandez

1 review  TT



May 28, 2024

The worst experience ever

After being with Telnix for a few years. They just block my account out of the blue with zero explanation. And I can't even ask why because their decision is final. This is clearly nonsensical, irrational, and illogical. And the best part is my personal information is stored on their account which is now blocked. Plus my funds. They were ok at the start but this experience has created a negative experience for me. Their support is the worst I have ever come across.

Date of experience: May 27, 2024



chris

12 reviews  GB



May 11, 2024

telnyx are a complete waste of time

I found impossible to sign up with telnyx - my account was blocked imediately, but they didn't tell me that - telnyx are a complete waste of time.

Date of experience: February 01, 2024

 Useful  Share



Reply from Telnyx

May 13, 2024

Hey! I know our anti-spam and anti-scams systems can occasionally catch an innocent bystander. If you'd like to send us your information for manual review, then I am happy to look more into it for you. Thanks!



chris

12 reviews  GB



Mar 12, 2024

abysmal

abysmal, almost worse than twilio and you have to try really hard to be worse than twilio. I can't review the actual service because like twilio it is impossible to get to the stage where you actually have a working account that is not immediately blocked.

Date of experience: March 01, 2024

 Useful

 Share



Reply from Telnyx

Mar 22, 2024

Hi Chris,

We are sorry to hear you are having issues logging into your account. Our recommendation would be to contact our support team via emailing support@telnyx.com vs. Live Chat and this will ensure that you will get connected to a member of our team who can assist you in getting back into your account.

Looking forward to resolving your issue!



prastar singh

1 review  IN



Nov 2, 2023

pathetic customer support service

pathetic customer support service. suspended my account for no reason. first, they will deduct money from your account automatically. then act like nothing has happened. they give you articles very bad, even google has better articles than Telnyx. do not waste your time please look for another service and recommend me other services pls.

Date of experience: November 02, 2023



Useful



Share



Reply from Telnyx

Jun 10, 2024

Hi Prastar,

Mark Morse Director of Customer Success here at Telnyx. We block/suspend accounts for many reasons to protect end users from potentially harmful fraudulent activity on our platform. If you would like an explanation of why your specific account was blocked, please reach out to support@telnyx.com and we would be happy to provide more context as to why your specific account was blocked.



niz niz

1 review HR



Jul 1, 2023

Strange company

I've bought a Belgium number, after activating it which took longtime already, i received email: account disabled for suspicious activity, i even didn't have any activity, luckily there was very small amount in the account, 😬

Date of experience: June 30, 2023

Useful 1 Share



Reply from Telnyx

Jan 29, 2024

Hi,

Mark Morse from the Customer Success team here at Telnyx. Unfortunately Trust Pilot doesn't give us an email or any account information for me to look up your account and why it got blocked for us to provide more perspective. Id be happy to look into this further if you email mark@telnyx.com.

Looking forward to working with you to resolve this matter!

EXHIBIT E

Telnyx Knows Nothing (fredposner.com)

12 points by kimi 17 days ago | hide | past | favorite | 4 comments

sunshine-o 17 days ago [-]

I had a very different experience with those providers: I has become impossible to use them for personal use because of the inefficient measures they set up.

- You can't register to Telnyx for personal use as an individual (anymore?)
- Twilio kicked me out after my first test call for suspicious activity
- voip.ms was the only one to have me but it simply doesn't work

In many countries telcos are really terrible and having an alternative number with a SIP account would be great. But now because of the robocall problem I can't have an account on any decent provider.

contactdq 16 days ago | parent | next [-]

Hi, co-founder/CEO of Telnyx here. I agree, the status quo sucks. We're trying to fix it, but as you can see, the regulators aren't very sympathetic to our cause.

Our mission has always been to democratize access to the power of the PSTN, and we've fought numerous battles (e.g., registered SMS) to make it easy for people to use our services and not be disadvantaged from other technologies (like pre-paid SIMs where no ID is required).

We are constantly trying to figure out ways to reduce friction for legitimate customers while preventing fraud on our platform, but increasingly, and especially with this NAL, we're being forced down a path of gatekeeping.

We don't think the FCC's decision was legally sound. It faces all sorts of challenges, including lack of statutory authority, violation of due process, and illegal rulemaking via enforcement, and we expect to challenge it in Appellate Court.

Pretty unhappy with Fred's post. Easy to play armchair quarterback.

This is not an easy problem to solve, and every step we take is an exercise in Type 1 vs Type 2 errors. Obviously, I think putting innocent people in prison (i.e. the blocking you experienced) is worse than letting a few guilty people free (i.e. bad actors through).

My LinkedIn post is here where you can read my full post, replies, and even some legal analysis:
https://www.linkedin.com/posts/dcasem_vague-rules-strictly-e...

supertrope 17 days ago | parent | prev [-]

I found Telnyx to be very difficult to use. KYC on sign-up including ID, face scan via app. Account locked upon sign up flow completion. A sales rep had to unlock it for me. Another round of KYC to add a payment method. A few days into testing the account was locked again. I decided to not port my numbers in.

contactdq 16 days ago | root | parent [-]

Sorry for this. I would appreciate if you could email me david [at] telnyx with your username, so we can figure out how to improve our systems.

Join us for [AI Startup School](#) this June 16-17 in San Francisco!

[Guidelines](#) | [FAQ](#) | [Lists](#) | [API](#) | [Security](#) | [Legal](#) | [Apply to YC](#) | [Contact](#)

Search:

EXHIBIT F

Order Short Name	Year	Fine	Total Calls	Days	Calls per Day	Fine per call	"High volume"	Language used	Spoofed	Call Type
Abramovich	2018	\$120,000,000*	96,758,223	90	1,075,091	\$ 1.24	Yes	"Massive volume"	Yes	Travel/Vacation
Roesel	2018	\$82,106,000	21,000,000	90	233,333	\$ 3.91	Yes	"Large volume"	Yes	Insurance
Moser	2020	\$9,997,750*	47,610	2	23,805	\$ 209.99	No	"Large-scale"	Yes	Election Interference
Rising Eagle	2021	\$225,000,000*	1,000,000,000	135	7,407,407	\$ 0.23	Yes	"Large volumes"	Yes	Insurance
Rhodes	2021	\$9,918,000* ¹	4,959	214	23	\$ 2,000.00	No	—	Yes	Racial Animus
Robbins (NAL)	2022	\$45,000,000	514,467	31	16,596	\$ 87.47	No	—	No	Insurance
Burkman	2023	\$5,134,500	1,141	∅ ²	—	\$ 4,500.00	No	—	No	Racial Animus / Election Interference
Sumco Panama	2023	\$299,997,000*	5,000,000,000	90	55,555,556	\$ 0.06	Yes	"Large volume"	Yes	Auto Warranty
Dorsher	2023	\$116,156,250*	9,763,599	60	162,727	\$ 11.90	No	—	No	Scam / TDoS
Kramer	2024	\$6,000,000	9,581	1	9,581	\$ 626.24	No	—	Yes	Election Interference
Lingo (NAL)	2024	\$2,000,000	3,978 ³	1	3,978	\$ 502.77³	No	—	Yes	Election Interference
Lingo (CD)	2024	\$1,000,000				\$ 251.38				Election Interference
Telnyx	2025	\$4,492,500	1,797 ⁴ 1,114	1	1,797 1,114	\$ 2,500.00 \$ 4,084.01	Yes	"High volume"	No	FCC & Family Targeted

*Indicates fine after upward adjustment for egregious conduct.

¹ Rhodes demonstrated that a number of calls were not spoofed, lowering the proposed forfeiture of \$12,910,000 to \$9,918,000 to reflect a \$1000 fine per call with a 100% upward adjustment. See [Rhodes Forfeiture Order](#), 36 FCC Rcd 705 (1), para. 54.

² FCC expressly refused to analyze number of days. See [Burkman Forfeiture Order](#), 38 FCC Rcd 5529 (6), para. 33.

³ FCC stated there was a total number of 9,581 calls with 3,978 of them originating from Lingo. If calculated using the total number of calls, the fine per call comes to \$208.75. See *In the Matter of Lingo Telecom, LLC*, File No.: EB-TCD-24-00036425, [Notice of Apparent Liability for Forfeiture](#) (May 23, 2024), paras. 9, 28.

⁴ 1,100 completed calls.

EXHIBIT G

Exhibit N

Comparison of Robocall Mitigation Database Filings

High-Level Know Your Customer (KYC) Practices				
	Information Collected	Information Validation	Contractual Provisions	Participation
Telnyx	(i) customer name, (ii) business email address, (iii) valid credit card information and other payment information, and (iv) physical address.	<ul style="list-style-type: none"> - IP address tracking - Payment method tracking - Scans for blacklisted IP addresses, blacklisted countries, blacklisted words in email names, blacklisted account names, new and repeated email addresses, disposable domains, and other fraud indicators - Scans of Do Not Originate list and Nomorobo for customer-provided numbers - Photo-based validation for high-risk accounts - Level 1 users heavily restricted to only 10 concurrent active calls - Enhanced KYC and due diligence efforts for customers seeking access to high-volume calls (i.e., Level 2 status) 	<ul style="list-style-type: none"> - AUP - Terms of Service - Privacy Policy - Immediate termination if customer fails to comply with any of the above policies. 	ITG and NANC
Selected Competitors				
Bandwidth	<i>Not discussed</i>	<ul style="list-style-type: none"> - Bandwidth tracks and records government enforcement actions and ever evolving industry trends to have up-to-date information on problematic use cases and known bad actors. - Consistently analyzes CDRs to identify problematic call patterns and their sources, and then incorporates these learnings into its traffic data analytics and detection technologies. 	Requires clear service-specific contractual requirements.	ITG and NANC
Grass-hopper	(i) name, (ii) telephone number, (iii) email address, (iv) business civic address, and (v) valid credit card information	<ul style="list-style-type: none"> - Operates a fraud prevention program that proactively monitors customer accounts for various indicia of potentially illegal or fraudulent activity. Some metrics lead to automatic account closure or outbound call blocking, whereas others result in accounts being flagged for further investigation or review. - Offers a free trial version of its service, which has a lower KYC threshold, but it has accordingly restricted free trial users to just 50 minutes of outbound calls. 	<ul style="list-style-type: none"> - AUP - Other associated online terms - Violation of these prohibitions constitute grounds for blocking or account termination 	ITG
Kirusa	<i>Not discussed</i>	<i>Not discussed</i>	<i>Not discussed</i>	<i>Not discussed</i>
Mitel	(i) name, (ii) address, and (iii) nature of business	Monitors traffic on a per customer and per ANI basis and takes action if and when traffic looks problematic or if Mitel receives complaints	Unified communications as a service (UCaaS) contract	<i>Not discussed</i>
Plivo	(i) “customer information,” (ii) the nature of their	Advanced in-house algorithm that detects and blocks potential fraudulent customers during the sign-up process. These users are granted access to Plivo services only after they provide	<ul style="list-style-type: none"> - AUP - Services may be suspended or terminated for violations 	<i>Not discussed</i>

	business, (iii) use case, and (iv) sign-up origin	details about their use case. Our fraud analysts review this information, and if all checks are passed, access is granted.		
Ring-Central	(i) legal name and (ii) contact details	<ul style="list-style-type: none"> - RingCentral uses analytics to help identify suspicious information. - RingCentral continuously monitors its network for suspicious activity. 	AUP	<i>Not discussed</i>
Signal Wire	(i) “detailed organizational information,” (ii) tax ID, and (iii) use case	<ul style="list-style-type: none"> - Follow NANC CATA Working Group best practices - Customers are limited to low call volumes at initial sign up. Customers who wish to receive higher call volumes are run through more stringent vetting procedures. 	<i>Not discussed</i>	<i>Not discussed</i>
Twilio	(i) legal business name, (ii) physical address, (iii) business type, (iv) business industry, (iv) business registration number, (vi) business regions of operation, (vii) website URL and social media profiles, and (viii) authorized representatives.	<ul style="list-style-type: none"> - Extensively investigates customers seeking access to high-volume origination services. - Customers that do not wish to provide all of the information in the “Information Collected” column will have their number of concurrent active calls heavily restricted - Verifies the information provided against public records and private databases and assesses KYC for fraud detection using common signals (e.g., email, phone number, IP addresses). 	<ul style="list-style-type: none"> - AUP - Terms of Service - Platform Agreements - Compliance team takes action if there is an identified failure to comply with any of the above policies. 	ITG and Alliance for Telecommunications Industry Solutions (ATIS)
Vonage	(i) names, (ii) addresses, (iii) verified e-mail address(es), (iv) verified phone number(s), (v) validated payment information; and If the customer is a legal entity: (a) the state or country of formation, (b) contact person, and (c) company registration number	<ul style="list-style-type: none"> - Proof of identity - Proof of residence - Proof of business legal entity - Proof of authorized individual 	<ul style="list-style-type: none"> - Terms of Service - Customer account may be terminated for violations 	NANC
Selected USTelecom Members				
Altafiber	(i) Type of business, (ii) state and country of incorporation,	<ul style="list-style-type: none"> - Security team identifies customers for further investigation - Review is aided by “external sources and internet searches” 	<ul style="list-style-type: none"> - AUP - Customer account can be terminated or suspended for repeated violations 	ITG
AT&T	(i) Government-issued identification, (ii) legal business name, (ii) federal tax	<ul style="list-style-type: none"> - Uses third party agencies to determine credit or fraud risk associated with the potential customer - Uses an identity theft prevention program 	<ul style="list-style-type: none"> - Service agreements - Customer account can be terminated for violations 	NANC

	identification or corporate charter number (iii) complete business address			
Big Bend Telecom (BBT)	<i>Not described in detail*</i> *Follows NANC CATA Working Group recommendations	<i>Not described in detail*</i> *Follows NANC CATA Working Group recommendations	<i>Not discussed</i>	<i>Not discussed</i>
Blackfoot Communications	<i>Not described in detail</i>	- Verification of credit history and business reputation Verification of identity	Non-described policies that allow for customer accounts to be suspended or terminated	ITG
Cal-Ore	<i>Not described in detail*</i> *Follows NANC CATA Working Group recommendations	<i>Not described in detail*</i> *Follows NANC CATA Working Group recommendations	- Terms and Conditions - Amends contracts, as appropriate, to prohibit illegal mass calling with the right to disconnect service	<i>Not discussed</i>
CL Tel	<i>Not described in detail*</i> *Follows NANC CATA Working Group recommendations	<i>Not described in detail*</i> *Follows NANC CATA Working Group recommendations	<i>Not discussed</i>	<i>Not discussed</i>
IronTon	(i) Address, (ii) service location, (iii) credit approval	<i>Not described in detail</i>	<i>Not discussed</i>	<i>Not discussed</i>
Union Springs Telephone Company	(i) SSN, (ii) date of birth, (iii) contact person for business (iv) address, (v) state or country of incorporation, (vi) federal tax ID	- New customers requesting “excessive” call paths will be screened - New and existing customers with “excessive” call paths receive outreach and educational materials - Call records and caller ID are reviewed	<i>Not discussed</i>	<i>Not discussed</i>
Verizon	<i>Not described in detail</i>	- Creates an anti-robocall score based on information collected - Follows the Anti-Robocall Principles published by the state attorneys general.	<i>Not discussed</i>	ITG and NANC
Ziply Fiber	<i>Not discussed</i>	<i>Not discussed</i>	<i>Not discussed</i>	<i>Not discussed</i>