Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	File No.: EB-TCD-24-00037170
Telnyx LLC	)	NAL/Acct. No.: 202432170009
	)	FRN: 0018998724

NOTICE OF APPARENT LIABILITY FOR FORFEITURE

Adopted: February 3, 2025 **Released: February 4, 2025**

By the Commission: Commissioner Simington dissenting and issuing a statement. Commissioner Gomez issuing a separate statement.

I. INTRODUCTION

1. We propose a penalty of $4,492,500 against Telnyx LLC (Telnyx or Company) for failing to take affirmative, effective measures to prevent malicious actors from using its network to originate illegal voice traffic.[1] Federal Communications Commission (FCC or Commission) staff and their family members, among others, were targeted with calls containing artificial and prerecorded voice messages that purported to be from a fictitious FCC "Fraud Prevention Team" as part of a government imposter scam aimed at fraudulently extracting payments of large amounts of money by intimidating recipients of the calls. All voice service providers are obligated to know their customers and exercise due diligence before allowing them to originate calls. As the providers responsible for introducing calls onto the public voice network, originating providers are best positioned to prevent illegal calls by stopping them before they begin. When a voice service provider fails to meet its obligations to properly vet its new or prospective customers before they commence using the provider's services to originate calls, it creates an opportunity for malicious actors to make illegal or unwanted calls that inflict harm on the American public. The penalty we propose today is part of the Commission's ongoing effort to hold voice service providers accountable for failing to protect their networks from illegal robocallers.

[1] Telnyx's filings with the Commission reflect its name is "Telnyx, LLC" while its incorporation documents reflect its name as "Telnyx LLC." Telnyx LLC (No. RMD0001645) Fed. Commc'ns Comm'n, Robocall Mitigation Database (filed Feb. 26, 2024) (Telnyx RMD Filing); Telnyx LLC FCC Form 499 Filer Information (2024); Illinois Secretary of State, Telnyx LLC Annual Report (filed July 17, 2024) (on file in EB-TCD-24-00036181) (Illinois Incorporation Filing). The Commission relies on the punctuation in the incorporation documents.

II. BACKGROUND

A. Legal Framework

2. Section 64.1200(n)(4) of the Commission's rules requires a voice service provider[2] to "[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."[3] The Commission does not mandate specific measures to comply with this rule, but rather provides that "[v]oice 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."[4] With regard to the know your customer (KYC) requirement of Section 64.1200(n)(4) in particular, such measures may include, for example, obtaining supporting records to verify the customer's identity, such as copies of government issued identification, corporate formation records, and third party records of a customer's physical address where the new customer will be using services that allow it to originate a significant volume of calls.[5] The Commission has "recommend[ed] that voice service providers exercise caution in granting access to high-volume origination services, to ensure that bad actors do not abuse such services"[6] and noted that voice service providers may need to "extensively investigate new customers seeking access to high-volume origination services."[7]

B. Relevant Parties

3. *Telnyx LLC*. Telnyx is a limited liability company registered in Illinois with its principal place of business in Chicago.[8] Telnyx sells various communications services, including a voice API service that allows users to "[m]ake, receive and control calls globally with programmable voice capabilities."[9] Telnyx is also a voice over internet protocol (VoIP) provider.[10] Telnyx "holds carrier status" in over 30 countries, including the United States, and offers "local calling in over 80 countries[,] and [public switched telephone network] replacement

---

[2] For purposes of this Notice of Apparent Liability, "voice service provider" means "any entity originating, carrying, or terminating voice calls through time-division multiplexing (TDM), Voice over Internet Protocol (VoIP), or commercial mobile radio service (CMRS)," unless otherwise noted. *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Fourth Report and Order, 35 FCC Rcd 15221, 15222, para. 2, n. 2 (2020) (*Fourth Call Blocking Order*).

[3] 47 CFR § 64.1200(n)(4) (emphasis added).

[4] *Fourth Call Blocking Order*, 35 FCC Rcd at 15233, para. 34.

[5] *See Lingo Telecom, LLC*, Order, DA 24-790, at Attach. 1 (Operating Procedures), § III, 2024 WL 3915892, at *12 (EB Aug. 21, 2024) (requiring use of these specific KYC procedures for "any customer who purchases a SIP Trunking Product").

[6] *Fourth Call Blocking Order*, 35 FCC Rcd at 15232, para. 32.

[7] *Id*. at 15233, para. 34.

[8] Illinois Incorporation Filing, *supra* note 1.

[9] Telnyx, *Voice API*, https://telnyx.com/products/voice-api (last visited Sept. 10, 2024).

[10] *See* Telnyx RMD Filing, *supra* note 1, at Attach. ("Telnyx LLC . . . is an interconnected voice over internet protocol ('VoIP') provider").

in [over] 45 [plus] markets."[11] Telnyx also holds a section 214 international authorization to provide facilities-based service and resale service from the Commission and has been granted direct access to numbering resources by the Commission.[12]

4. *MarioCop Account Holders.*[13] On February 6, 2024, Telnyx accepted a new customer from whom it collected the following information, purportedly for the purpose of knowing who the customer is: the name Christian Mitchell, an email address using the domain @mariocop123.com, an IP address from Edinburgh, Scotland, and a physical address in Toronto, Canada, associated with a Sheraton hotel (First MarioCop Account).[14] Also on February 6, 2024, Telnyx accepted a new customer for whom it collected the following information: the name Henry Walker, an email address also using the domain @mariocop123.com, an IP address from London, England, and the same physical address in Toronto associated with the same Sheraton hotel (Second MarioCop Account).[15] The following table summarizes the profile of each account (together, MarioCop Accounts):

Account	**First MarioCop Account**	**Second MarioCop Account**
Name	Christian Mitchell	Henry Walker
Email	christian@mariocop123.com	henry@mariocop123.com
IP Address	84.247.40.137 (Edinburgh, Scotland)	185.137.36.183 (London, England)
Address	123 Queen St W, Toronto, ON M5H 3M9, Canada	123 Queen St W, Toronto, ON M5H 3M9, Canada

[11] Telnyx, *Global Coverage*, https://telnyx.com/global-coverage (last visited Sept. 17, 2024).

[12] *See International Authorizations Granted: Section 214 Applications (47 C.F.R. § 63.18); Section 310(B)(4) Requests*, DA 11-837, Public Notice, 26 FCC Rcd 6697 (IB 2011) (*Section 214 Authorizations*) (granting Telnyx's application for authority to provide facilities-based service in accordance with section 63.18(e)(1) and resale service in accordance with section 63.18(e)(2) of the Commission's rules); *Notice of Interconnected VOIP Numbering Authorization Granted*, WC Docket No. 16-172, Public Notice, 31 FCC Rcd 7700 (2016).

[13] Although we refer to two MarioCop accounts, it is possible that one person was operating both accounts. However, the Bureau is unable to confirm this because of Telnyx's KYC measures.

[14] Telnyx Subpoena Response (Mar. 20, 2024) (on file in EB-TCD-24-00036181) (Telnyx Mar. 20 Subpoena Response), at Response to Request for Documents (RFD) No. 2; WhatIsMyIPAddress.com, *IP Details For: 84.257.40.137*, https://whatismyipaddress.com/ip/84.247.40.137 (last visited Aug. 27, 2024) (showing the IP address in Edinburgh); Sheraton, Sheraton Centre Toronto Hotel, https://www.marriott.com/en-us/hotels/yyztc-sheraton-centre-toronto-hotel/overview/ (last visited Sept. 20, 2024) (identifying address as 123 Queen St W, Toronto, Canada) (Sheraton).

[15] Telnyx Subpoena Response (Aug. 16, 2024) (on file in EB-TCD-24-00036181) (Telnyx Aug. 16 Subpoena Response), Response to Request for Information (RFI) No. 1; WhatIsMyIPAddress.com, *IP Details For: 185.137.36.183*, https://whatismyipaddress.com/ip/185.137A.36.183 (last visited Aug. 27, 2024) (showing the IP address in London); *see* Sheraton.

C. Factual Background

5. *The FCC Imposter Calls.* On the night of February 6, 2024, and continuing into the morning of February 7, 2024, over a dozen FCC staff and some of their family members reported receiving calls on their personal and work telephone numbers that transmitted the following artificial and prerecorded voice message (Imposter Calls):[16]

> Hello [first name of recipient] you are receiving an automated call from the Federal Communications Commission notifying you the Fraud Prevention Team would like to speak with you. If you are available to speak now please press one. If you prefer to schedule a call back please press two.[17]

The FCC has no such "Fraud Prevention Team" and the FCC was not responsible for these calls. Nor does the FCC publish or otherwise share staff personal phone numbers. It remains unclear how these individuals were targeted. The purpose of the calls appears to have been to threaten, intimidate and defraud. One recipient of an Imposter Call reported that they were ultimately connected to someone who "demand[ed] that [they] pay the FCC $1000 in Google gift cards to avoid jail time for [their] crimes against the state."[18]

6. *The Enforcement Bureau's Investigation.* The FCC's Enforcement Bureau (Bureau) obtained details pertaining to eight calls that reached Commission staff and worked with the Industry Traceback Group (ITG) to use this information to trace the source of the calls.[19] The ITG is the registered consortium selected by the Bureau to lead industry efforts to trace back suspected illegal robocalls to determine their origination.[20] With respect to the Imposter Calls, the ITG determined that Telnyx was the originating voice service provider.[21] Telnyx, in turn, identified the First MarioCop Account as its customer responsible for placing the calls, and subsequently identified the Second MarioCop Account because it shared {[ ]} with the First MarioCop Account.[22]

---

[16] YouMail, Analysis Report of the FCC Imposter Calls (2024) (on file in EB-TCD-24-00036181).

[17] Voicemail-10752090176 (on file in EB-TCD-24-00036181); *see, e.g.*, Email from {[ ]}, to Security Operations Center, FCC (Feb. 7, 2024, 11:44 EDT); Email from {[ ]}, to Security Operations Center, FCC (Feb. 7, 2024, 10:32 EDT); Email from {[ ]}. Material set off by double brackets {[ ]} is confidential and is redacted from the public version of this document.

[18] YouMail, Report for (888) 580-0091 (on file in EB-TCD-24-00036181) (listing a report filed on Feb. 6, 2024 complaining about a robocall received from telephone number (888) 580-0091 from the "Federal Communication Commission Fraud Committee") (last visited Sept. 17, 2024).

[19] *See* ITG, Traceback Report (Feb. 12, 2024) (on file in EB-TCD-24-00036181) (Traceback Report).

[20] *Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, EB Docket No. 20-22, Report and Order, 38 FCC Rcd 7561, 7561-62, para. 1 (EB 2023).

[21] *See* Traceback Report.

[22] *Id.*; Telnyx Aug. 16 Subpoena Response, *supra* note 15, Response to RFI No. 2(4).

7. The Bureau subpoenaed Telnyx for information about the calls placed by the MarioCop Accounts.[23] The First MarioCop Account purchased two phone numbers, outbound call termination services {[ ]}, and programmable voice services from Telnyx.[24] Call detail records produced by Telnyx show that between February 6, 2024 and February 7, 2024—the timeframe FCC staff and their family members reported receiving the Imposter Calls—the First MarioCop Account made 1,029 outbound calls.[25] The Second MarioCop Account also made at least 768 calls on February 6, 2024.[26]

8. In the course of routine examination of new users, Telnyx flagged the First MarioCop Account for further internal investigation due to {[ ]}.[27] On February 7, 2024, Telnyx terminated the First MarioCop Account after determining the nature of its calls violated Telnyx's terms and conditions and acceptable use policy.[28] {[ ]}.[29] Telnyx then reported the First MarioCop Account to the Commission.[30]

9. The Bureau also subpoenaed Telnyx for information that would identify the owners of the MarioCop Accounts. Working with all the information Telnyx provided, the Bureau determined that the very limited identifying information Telnyx collected from its customer was false. The Bureau was unable to identify the person who opened either account. The name Christian Mitchell is not associated with the address in Toronto, which is the address of a Sheraton hotel.[31] The @mariocop123.com domain is not associated with any known business; a website using the same domain was created in February 2024 and remains undeveloped.[32] The IP address for the First MarioCop Account was from Edinburgh, Scotland and was not affiliated with the physical Toronto address.[33] Similarly, with respect to the Second MarioCop Account, the Bureau was unable to identify anyone named Henry Walker associated

---

[23] Subpoena to Telnyx (Feb. 9, 2024) (on file in EB-TCD-24-00036181); Subpoena to Telnyx (Feb. 27, 2024) (on file in EB-TCD-24-00036181); Subpoena to Telnyx (Mar. 5, 2024) (on file in EB-TCD-24-00036181); Subpoena to Telnyx (Aug. 2, 2024) (on file in EB-TCD-24-00036181).

[24] Telnyx Mar. 20 Subpoena Response, *supra* note 14, at Response to RFI No. 2; Telnyx Subpoena Response (June 6, 2024) (on file in EB-TCD-24-00036181) (Telnyx June 6 Subpoena Response) at Response No. I(3);

[25] Telnyx Mar. 20 Subpoena Response, *supra* note 14, at Attach. A.

[26] Telnyx Aug. 16 Subpoena Response, *supra* note 15, at Attach. A.

[27] Telnyx June 6 Subpoena Response, at Response No. I(4).

[28] *Id.*, at Response No. I(5).

[29] Telnyx Aug. 16 Subpoena Response, *supra* note 15, at Response to RFI No. 2(4).

[30] Email from {[ ]} (Feb. 7, 2024 6:51 PM EDT) (on file in EB-TCD-24-00036181) ({[ ]} Email).

[31] *See* Sheraton, *supra* note 14.

[32] *See Mariocop123*.com, http://www.mariocop123.com/ (last visited Sept. 11, 2024); Google, *About the source: mariocop123.com*, https://www.google.com/search?q=About+http://www.mariocop123.com/&tbm=ilp&ctx=atr&sa=X&ved=2ahUKEwiW0JCU0LuIAxVvCFkFHVtbKicQv5AHegQIABAC (last visited Sept. 11, 2024) (stating the website was first indexed by Google in February 2024).

[33] WhatIsMyIPAddress.com, *IP Details For: 84.257.40.137*, https://whatismyipaddress.com/ip/84.247.40.137 (last visited Aug. 27, 2024) (showing the IP address in Edinburgh).

with the address in Toronto. The Second MarioCop Account's use of the mariocop123.com domain did not reveal anything about its business affiliations and the IP address affiliated with the Second MarioCop Account was from London, England, not Toronto.[34] Both accounts paid Telnyx in Bitcoin.[35] The Bitcoin transaction ID and wallet address the MarioCop Accounts used to pay Telnyx were anonymized and could not be traced.[36]

10. *Telnyx's KYC Measures*. Before opening the MarioCop Accounts, Telnyx collected a name, non-free email address, physical address, and IP address from each applicant.[37] {[ ]},[38] neither of the MarioCop Account applicants provided a telephone number.[39] Telnyx required the applicants to {[ ]},[40] but accepted the names and physical addresses at face value, without any further requests for corroboration or independent verification.[41] Telnyx verified that {[ ]}.[42] {[ ]}.[43] The reports generated by Telnyx's third party vendor estimated that the First MarioCop Account {]}.[45] Additionally, {[

[34] *See* Telnyx Aug. 16 Subpoena Response, *supra* note 15, at Response to RFI No. 1 (showing the Second MarioCop Account's physical address as 123 Queen St W, Toronto, Canada, which is associated with the Sheraton Toronto); WhatIsMyIPAddress.com, *IP Details For: 185.137.36.183*, https://whatismyipaddress.com/ip/185.137.36.183 (last visited Aug. 27, 2024) (showing the IP address in London).

[35] Telnyx Mar. 20 Subpoena Response, *supra* note 14, at Response to RFD No. 2; Telnyx Aug. 16 Subpoena Response, *supra* note 15, at Response to RFI No. 7.

[36] *See* Telnyx Mar. 20 Subpoena Response, *supra* note 14, at Response to RFD No. 2; Telnyx Aug. 16 Subpoena Response, *supra* note 15, at Response to RFI No. 7 (showing the Second MarioCop account's Bitcoin transaction ID).

[37] Telnyx Mar. 20 Subpoena Response, *supra* note 14, at Response to RFD No. 2; Telnyx Aug. 16 Subpoena Response, *supra* note 15, at Response to RFI No. 1.

[38] Telnyx Subpoena Response (Mar. 13, 2024) (on file in EB-TCD-24-00036181) (Telnyx Mar. 13 Subpoena Response) ("Customer Verification" bullet).

[39] Telnyx Mar. 20 Subpoena Response, *supra* note 14, at Response to RFD No. 2; Telnyx Aug. 16 Subpoena Response, *supra* note 15, at Response to RFI No. 1.

[40] Telnyx June 6 Subpoena Response, *supra* note 24, at Response No. I(3); Telnyx Aug. 16 Subpoena Response, *supra* note 15, at Response to RFI No. 2(3).

[41] Telnyx Mar. 13 Subpoena Response (identifying no process for verifying names or physical addresses).

[42] Telnyx June 6 Subpoena Response, *supra* note 24, at Response No. I(4); Telnyx Aug. 16 Subpoena Response, *supra* note 15, at Response to RFI No. 2(4).

[43] Telnyx June 6 Subpoena Response, *supra* note 24, at Response No. I(2); Telnyx Aug. 16 Subpoena Response, *supra* note 15, at Response to RFI No. 2(2).

[44] Telnyx Aug. 16 Subpoena Response, *supra* note 15, at Attach. B-C.

[45] *Id.* at Attach. B.

]}.[46] Telnyx concluded the two applicants' profiles {[ ]} so Telnyx permitted the MarioCop Accounts to be created, which allowed the new customers to make {[ ]} from each account.[47] Telnyx took no other steps to verify the identity of the persons behind the MarioCop Accounts or their purpose in establishing accounts with Telnyx.

III. DISCUSSION

A. Telnyx Did Not Know the MarioCop Account Holders

11. A voice service provider must "[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."[48] All voice service providers must, at a minimum, "know their customers and take measures that have the effect of actually restricting the ability of new and renewing customers to originate illegal traffic."[49] Measures that may contribute to satisfying the KYC obligation include, for example, obtaining supporting records to verify the customer's identity such as copies of government issued identification, corporate formation records, proof of good standing, a federal employer identification number or business registration number, an active telephone number, third party records of a customer's physical address, type of goods or services offered, and verification of commercial presence.[50] Moreover, 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, noting that "voice service providers may extensively investigate new customers seeking access to high-volume origination services."[51]

12. Telnyx is a voice service provider and was therefore legally obligated under the Commission's rules to take affirmative, effective measures to prevent new customers from using its network to originate illegal calls, including knowing its customers.[52] Telnyx failed to conduct a sufficient inquiry into the MarioCop Account holders before allowing them to start originating {[ ]} calls, which allowed the account holders to put fraudulent imposter calls on the network in a short period of time, many of which targeted FCC staff members and their families.[53] *First*, Telnyx collected very limited information about the MarioCop Account

---

[46] Telnyx Aug. 16 Subpoena Response, *supra* note 15, at Attach. B-C (showing the third-party service's review of the MarioCop accounts).

[47] Telnyx June 6 Subpoena Response, *supra* note 24, at No. I(3); Telnyx Aug. 16 Subpoena Response, *supra* note 15, at Response to RFI No. 2(3).

[48] 47 CFR § 64.1200(n)(4).

[49] *Fourth Call Blocking Order*, *supra* note 2, at 15233, para. 34.

[50] *See Lingo Telecom, LLC*, Order, DA 24-790, at Attach. 1 (Operating Procedures), § III, 2024 WL 3915892, at *12 (EB Aug. 21, 2024) (requiring use of these specific KYC procedures for "any customer who purchases a SIP Trunking Product").

[51] *Fourth Call Blocking Order*, *supra* note 2, at 15233, para. 34.

[52] *See* 47 CFR § 64.1200(n)(4); *Fourth Call Blocking Order*, 35 FCC Rcd 15221, 15222, para. 2, n. 2 (2020); *see supra* para. 3 (explaining Telnyx offers VoIP services).

[53] *See supra* paras. 5, 10.

applicants. It collected only a name, email address, physical address, and IP address.[54] It did not collect a phone number from either applicant.[55]

13. *Second*, with the exception of {[ ]}, Telnyx made no attempt to discern whether the limited amount of identifying information its customer provided was legitimate and it overlooked obvious discrepancies in the information it collected.[56]

14. *Third*, Telnyx's third-party vendor {[ ]}.[57] The MarioCop Account applicants provided a physical address in one country (Canada) but provided an IP address from a different country (Scotland or England).[58] Moreover, the steps that Telnyx took—{[ ]}—did nothing to verify the identities of the MarioCop Account applicants.[59] As a result of not verifying the limited information it collected, Telnyx's {[ ]} was essentially ineffective; the service indicated merely that the fake identities {[ ]}.[60]

15. *Fourth*, Telnyx ignored the red flags that its {[ ]}.[61] There may be reasonable and legitimate reasons for having {[ ]}, but this may also raise the possibility that the customer is attempting to hide its true identity and has created a {[ ]} for the sole purpose of anonymously placing illegal robocalls. Although not a basis for our finding of apparent violations in this case, we note that Telnyx accepted Bitcoin as payment for the MarioCop Accounts, which further helped the account holders to conceal their identities.[62] Telnyx's remaining onboarding procedures, requiring agreement to certain policies, did nothing to help Telnyx better know who was behind the MarioCop Accounts.[63] Becoming Telnyx's customer and gaining access to outbound calling services that allowed origination of hundreds of calls (more than 1,000 calls from the First

[54] *See supra* para. 10.

[55] *See id*.

[56] *See id.*

[57] Telnyx Aug. 16 Subpoena Response, *supra* note 15, at Attach. B-C (showing the third-party service's review of the MarioCop accounts).

[58] *See id.*

[59] *See supra* para. 10.

[60] *See id.*

[61] *See id.*

[62] *See* Telnyx Mar. 20 Subpoena Response, *supra* note 14, at Response to RFD No. 2; Telnyx Aug. 16 Subpoena Response, *supra* note 15, at Response to RFI No. 7.

[63] *See supra* para. 10.

MarioCop Account) was as simple as making up a fake name and address and acquiring a non-free email address.

16. Our rules require Telnyx to know its customers.[64] Yet it did not know who the MarioCop Account holders were. We therefore conclude that Telnyx apparently violated section 64.1200(n)(4) of our rules by allowing the First MarioCop Account and the Second MarioCop Account access to outbound calling services without actually knowing the true identities of the account holders.[65] By extension, we believe we could likely find that Telnyx apparently violated our rules with regards to every customer it onboarded using the same process as it did for the MarioCop Accounts. We decline to do so here absent further investigation.

B. Proposed Forfeiture

17. We find that Telnyx apparently willfully and repeatedly violated section 64.1200(n)(4) of the Commission's rules by failing to know its customers. We propose a $4,492,500 forfeiture.

18. Section 503(b) of the Communications Act of 1934, as amended (the Act), authorizes the Commission to impose a forfeiture against any entity that "willfully or repeatedly failed to comply with any of the provisions of [the] Act or of any rule, regulation, or order issued by the Commission."[66] We may proceed directly to issuing an NAL without first issuing a citation because Telnyx has 214 authority and its Robocall Mitigation Database (RMD) filing constitutes a "license, permit, certificate, or other authorization issued by the Commission."[67]

19. In exercising our forfeiture authority, we are subject to statutory limits on the amount of any forfeiture assessed.[68] To assess a proposed forfeiture, we first determine the applicable base forfeiture. We then consider the "nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require."[69] We may adjust a forfeiture upward or downward based on various criteria, such as whether violations are egregious, intentional, repeated, cause substantial harm, generate substantial economic gain for

[64] 47 CFR § 64.1200(n)(4); *see* Telnyx RMD Filing, *supra* note 1, at Attach. A (identifying itself as a VoIP provider).

[65] *See id.*

[66] 47 U.S.C. § 503(b)(1)(B).

[67] *Id.* § 503(b)(5); *see* Telnyx RMD Filing, *supra* note 1; *see also Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573, 2608, para. 70 (2023) (*Sixth Caller ID Authentication Order*) (finding a certification as a result of being registered in the Robocall Mitigation Database is a Commission authorization).

[68] 47 U.S.C. § 503(b)(2); 47 CFR § 1.80(b)(2). The maximum forfeiture amounts stated in section 1.80(b) of our rules reflect adjustments to the statutory caps in section 503(b)(2) to reflect inflation. *See generally Amendment of Section 1.80(b) of the Commission's Rules, Adjustment of Civil Monetary Penalties to Reflect Inflation*, Order, DA 25-5 (EB 2025); *see also Annual Adjustment of Civil Monetary Penalties to Reflect Inflation*, 90 Fed. Reg. 3710 (Jan. 15, 2025) (setting January 15, 2024 as the beginning date for the application of the increased amounts).

[69] 47 U.S.C. § 503(b)(2)(E); 47 CFR § 1.80(b)(11), Note 2 to paragraph (b)(11).

the violator, or whether the violations are voluntarily disclosed.[70] The base forfeiture, with any adjustment, is then multiplied by the number of violations to determine the proposed forfeiture.

20. *Applicable Statutory Limitation on the Forfeiture.* Common carriers are subject to a maximum forfeiture of $251,322 per violation.[71] A common carrier includes "any person engaged as a common carrier for hire, in interstate or foreign communications by wire[.]"[72] Telnyx applied for, and was granted, an international section 214 authorization by the Commission in 2011.[73] That grant authorized Telnyx "to become a facilities-based international common carrier" and "to become a resale-based international common carrier."[74] We therefore find Telnyx is a common carrier and is subject to a maximum forfeiture of $251,322 per violation.[75]

21. *Base Forfeiture.* Neither the Commission's forfeiture guidelines nor its case law establishes a base forfeiture for violations of section 64.1200(n)(4). To determine an appropriate base forfeiture, we look to the base forfeiture established for an analogous violation.[76]

22. We find a violation of section 64.6305(g)(1) comparable to the violation here and that the penalty for violating section 64.6305(g)(1) is an appropriate proxy. Section 64.6305(g)(1) prohibits intermediate providers and voice service providers from accepting traffic directly from a domestic voice service provider that does not have a filing in the RMD.[77] The Commission established the RMD as a publicly available database to aid in monitoring compliance with the FCC's caller ID authentication and robocall mitigation rules and to facilitate enforcement action.[78] To promote transparency and effective robocall mitigation, the Commission requires all voice service providers to file certifications in the RMD detailing their efforts to stem the origination of illegal robocalls on their networks.[79] Accordingly, an

---

[70] 47 CFR § 1.80(b)(11), Tbl. 3 to paragraph (b)(11) (adjustment criteria for section 503 forfeitures).

[71] 47 CFR § 1.80(b)(2).

[72] 47 U.S.C. § 153(11).

[73] *Section 214 Authorizations*, 26 FCC Rcd at 6697 (applying for authority for Telnyx to provide facilities-based service in accordance with section 63.18(e)(1) and resale service in accordance with section 63.18(e)(2) of the Commission's rules); *see also* 47 CFR § 63.18 ("[A]ny party seeking authority pursuant to Section 214 of the Communications Act of 1934, as amended, to construct a new line, or acquire or operate any line, or engage in transmission over or by means of such additional line for the provision of common carrier communications services between the United States, its territories, or possessions, and a foreign point *shall request* such authority by formal application." (emphasis added)).

[74] *Section 214 Authorizations*, 25 FCC Rcd at 6697.

[75] 47 CFR § 1.80(b)(2).

[76] *Hawaiian Telcom Services Co. v. Nexstar Media Inc.*, MB Docket No. 23-228, Memorandum Opinion and Order and Notice of Apparent Liability for Forfeiture, DA 24-116, 2024 WL 519155, at *6, para. 17, (MB Feb. 7, 2024) ("In cases where [the Commission] has not established a base forfeiture amount for an apparent violation, it has looked to forfeitures issued in analogous cases for guidance.").

[77] 47 CFR § 64.6305(g)(1).

[78] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1903, para. 83 (2020) (*Second Caller ID Authentication Order*).

[79] *Id.* at para 82; *Sixth Caller ID Authentication Order*, *supra* note 67, at 2592-93, para. 37 (expanding the obligation to file a robocall mitigation plan along with a certification in the Robocall Mitigation Database to all providers in the call path).

intermediate provider or voice service provider must confirm its directly upstream domestic voice service provider has a filing in the RMD before accepting traffic from that provider.[80] The purpose of this rule is to ensure providers have adequate robocall mitigation practices before gaining access to the U.S. voice network.[81]

23. The Commission has found that "aggressive penalties are appropriate" for providers who accept traffic in violation of section 64.6305(g)(1).[82] Blocking the sources of illegal robocalls "is an important tool for protecting American consumers from illegal robocalls."[83] "[I]llegal robocalls cause significant consumer harm" and "[p]enalties for failure to comply with mandatory blocking requirements must deter noncompliance and be sufficient to ensure that entities subject to these requirements are unwilling to risk suffering serious economic harm."[84] Accordingly, the Commission set a base forfeiture of $2,500 per call for any calls transmitted as a result of a violation of section 64.6305(g)(1).[85]

24. We find that a provider's duty to know its customer is analogous to its duty to know whether its directly upstream domestic voice service provider has a filing in the RMD. Both obligations require a provider to conduct a certain amount of due diligence on the party from which it receives traffic.[86] Both obligations exist to protect the U.S. voice network and consumers from illegal robocalls.[87] A provider's decision to onboard a new customer without knowing that customer or to accept traffic from a provider that does not have a filing in the RMD potentially increases the chances that consumers are flooded with illegal robocalls. Both failures can result in significant consumer harm.[88] Accordingly, like penalties calculated under 64.6305(g)(1), we calculate the penalty under 64.1200(n)(4) by considering the number of calls accepted from the customer.

25. We also consider the "nature, circumstances, extent, and gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to

[80] 47 CFR § 64.6305(g)(1).

[81] *Second Caller ID Authentication Order*, 36 FCC Rcd at 1905, para. 87.

[82] *See Sixth Caller ID Authentication Order*, *supra* note 67, at 2601, para. 54.

[83] *See id.* at 2601-02.

[84] *See id.*

[85] *See id.* at 2602, para. 55; 47 CFR § 1.80(b)(11) Tbl. 1.

[86] *See* 47 CFR §§ 64.1200(n)(4); 64.6305(g)(1); s*ee also Second Caller ID Authentication Order*, *supra* note 78, at 1905, para. 87 ("as voice service providers monitor the database to ensure they remain compliant with our rules, they must necessarily review the listing of voice service providers with which they interconnect to ensure that such certifications are sufficient.").

[87] *See Second Caller ID Authentication Order*, *supra* note 78, at 1906, para. 89 ("We find the rule we establish . . . best leverages the role of intermediate providers to combat illegal robocalls within our greater robocall mitigation scheme."); *Fourth Call Blocking Order*, *supra* note 2, at 15232, para. 33 ("When originating and gateway providers stop these calls in the first instance, it ensures that illegal traffic never enters the network, let alone reaches consumers.").

[88] *See* Fed. Trade Comm'n, Consumer Sentinel Network Data Book 2023 at 12 (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf (reporting 297,765 complaints of telephone fraud amounting to $850 million in losses in 2023).

pay, and such other matters as justice may require."[89] The responsibility imposed by section 64.1200(n)(4) for providers to know their customers is a critical aspect of protecting Americans from illegal and harmful robocalls.[90] With respect to this important obligation, Telnyx had no effective KYC measures in place and took no meaningful steps to learn who was behind the MarioCop Accounts.[91] {[

]}.[92] As a result of Telnyx's misconduct, over a dozen FCC employees and hundreds of others, received a barrage of illegal and deceptive calls designed to defraud them.[93]

26. We apply a base forfeiture of $2,500 per call to the 1,797 calls that Telnyx allowed the MarioCop Accounts to make here. This renders a $4,492,500 total base forfeiture for allowing the MarioCop Accounts to make 1,797 calls.[94]

27. After balancing the section 503 statutory factors, consistent with the *Forfeiture Policy Statement*, and considering the totality of the circumstances, we decline to apply either an upward or downward adjustment of the $4,492,500 base forfeiture.[95] However, we find there are factors supporting an upward adjustment for egregiousness and substantial harm.[96] Telnyx provided the MarioCop Accounts with access to the U.S. network without actually knowing or confirming anything about the customers other than that they had {[

]}.[97] Telnyx never verified the MarioCop Account holders' actual names, addresses, business, or purpose for establishing accounts.[98] Telnyx never inquired further when {[

]}.[99] As a result, the First MarioCop Account used Telnyx's network to make illegal robocalls impersonating the FCC and to intimidate and deceive call recipients.[100] "[B]oth Congress and

---

[89] 47 U.S.C. § 503(b)(2)(E).

[90] *See Fourth Call Blocking Order*, *supra* note 2, at 15232, para. 33.

[91] *See supra* para. 10.

[92] *See id*.

[93] *Supra* paras. 5, 7.

[94] *See* 47 CFR § 64.1200(n)(4).

[95] *See id.* § 1.80(b)(11), Note 2 to paragraph (B)(11); *Commission's Forfeiture Policy Statement and Amendment of Section 1.80 of the Rules to Incorporate the Forfeiture Guidelines*, 12 FCC Rcd 17087, 17101, para. 27 (1997) (*Forfeiture Policy Statement*) ("[A]lthough the base amount is the starting point in assessing a forfeiture, the forfeiture may be . . . increased to the statutory maximum when the adjustment criteria are considered based on the facts of the case."); *see, e.g.*, *ScammerBlaster Notice of Apparent Liability*, 37 FCC Rcd 8988, 8998-99, paras. 23-26 (2022).

[96] *See* 47 U.S.C. § 503(b)(2)(E); 47 CFR § 1.80(b)(11), Tbl. 3.

[97] *Supra* para. 10.

[98] *See id.*

[99] *See id.*

[100] *See supra* para. 16.

the Commission have long recognized that the placement of illegal robocalls causes consumers significant harm, including that such calls are a nuisance and invasion of privacy."[101] Such calls impersonating a business or government agency pose significant risk to consumers.[102] These considerations would weigh in favor of an upward adjustment.[103] However, in light of Telnyx's prompt disclosure to the Commission that it had originated these calls, we decline to apply an upward adjustment. We encourage parties to continue to work with the Commission early on and to disclose potential violations.[104]

28. Therefore, after applying the statutory factors, section 1.80 of the Commission's rules, and the *Forfeiture Policy Statement*, we propose a total forfeiture of $4,492,500 for Telnyx's failure to comply with section 64.1200(n)(4).[105]

IV. CONCLUSION

29. We have determined that Telnyx apparently willfully and repeatedly violated section 64.1200(n)(4) of the Commission's rules. As such, Telnyx is apparently liable for a forfeiture of $4,492,500.

V. ORDERING CLAUSES

30. Accordingly, **IT IS ORDERED** that, pursuant to section 503(b) of the Act, 47 U.S.C. § 503(b), and section 1.80 of the Commission's rules, 47 CFR § 1.80, Telnyx LLC is hereby **NOTIFIED** of this **APPARENT LIABILITY FOR A FORFEITURE** in the amount of four million four hundred ninety two five hundred dollars ($4,492,500) for willful and repeated violations of section 64.1200(n)(4) of the Commission's rules, 47 CFR § 64.1200(n)(4).

31. **IT IS FURTHER ORDERED** that, pursuant to section 1.80 of the Commission's rules, 47 CFR § 1.80, within thirty (30) calendar days of the release date of this Notice of Apparent Liability for Forfeiture, Telnyx LLC **SHALL PAY** the full amount of the proposed forfeiture or **SHALL FILE** a written statement seeking reduction or cancellation of the proposed forfeiture consistent with paragraph 34 below.

---

[101] *Best Insurance Contracts, Inc., and Philip Roesel, Dba Wilmington Insurance Quotes*, Forfeiture Order, 33 FCC Recd 9204, 9219, para. 40 (2018). At least some of the Imposter Calls reached cell phones. Traceback Report, *supra* note 19. Telnyx offered no evidence of consent. *Id.* Accordingly, the calls were illegal. *See* 47 CFR § 64.1200(a)(1) (prohibiting calls to cellphones containing artificial or prerecorded voice messages absent an emergency purpose or prior express consent).

[102] *See* Fed. Trade Comm'n, *Impersonation scams: not what they used to be* (Apr. 1, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/imposter-scams-spotlight-2024.pdf ("In 2023, data from the FTC alone show more than 330,000 reports of business impersonation scams and nearly 160,000 reports of government impersonation scams. . . . Combined, reported losses to these impersonation scams topped $1.1 billion for the year[.]").

[103] *See* 47 CFR § 1.80(b)(11), Tbl. 3.

[104] *See id.*; {[ ]} Email, *supra* note 30.

[105] *See* 47 U.S.C. § 503(b)(2)(B); 47 CFR § 1.80(b)(11); *Forfeiture Policy Statement*, 12 FCC Rcd at 17101, para. 27. Any entity that is a "Small Business Concern" as defined in the Small Business Act (Pub. L. 85-536, as amended) may avail itself of rights set forth in that Act, including rights set forth in 15 U.S.C. § 657, "Oversight of Regulatory Enforcement," in addition to other rights set forth herein.

32. In order for Telnyx LLC to pay the proposed forfeiture, Telnyx LLC shall notify Lisa Ford at Lisa.Ford@fcc.gov of its intent to pay, whereupon an invoice will be posted in the Commission's Registration System (CORES) at https://apps.fcc.gov/cores/userLogin.do. Upon payment, Telnyx LLC shall send electronic notification of payment to Lisa Ford, Enforcement Bureau, Federal Communications Commission, at Lisa.Ford@fcc.gov on the date said payment is made. Payment of the forfeiture must be made by credit card using CORES at https://apps.fcc.gov/cores/userLogin.do, ACH (Automated Clearing House) debit from a bank account, or by wire transfer from a bank account. The Commission no longer accepts forfeiture payments by check or money order. Below are instructions that payors should follow based on the form of payment selected:[106]

- Payment by wire transfer must be made to ABA Number 021030004, receiving bank TREAS/NYC, and Account Number 27000001. In the OBI field, enter the FRN(s) captioned above and the letters "FORF". In addition, a completed Form 159[107] or printed CORES form[108] must be faxed to the Federal Communications Commission at 202-418-2843 or e-mailed to RROGWireFaxes@fcc.gov on the same business day the wire transfer is initiated. Failure to provide all required information in Form 159 or CORES may result in payment not being recognized as having been received. When completing FCC Form 159 or CORES, enter the Account Number in block number 23A (call sign/other ID), enter the letters "FORF" in block number 24A (payment type code), and enter in block number 11 the FRN(s) captioned above (Payor FRN).[109] For additional detail and wire transfer instructions, go to https://www.fcc.gov/licensing-databases/fees/wire-transfer.
- Payment by credit card must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by credit card, log-in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" from the CORES Menu, then select FRN Financial and the view/make payments option next to the FRN. Select the "Open Bills" tab and find the bill number associated with the NAL Acct. No. The bill number is the NAL Acct. No. with the first two digits excluded (e.g., NAL 1912345678 would be associated with FCC Bill Number 12345678). After selecting the bill for payment, choose the "Pay by Credit Card" option. Please note that there is a $24,999.99 limit on credit card transactions.
- Payment by ACH must be made by using CORES at https://apps.fcc.gov/cores/userLogin.do. To pay by ACH, log in using the FCC Username associated to the FRN captioned above. If payment must be split across FRNs, complete this process for each FRN. Next, select "Manage Existing FRNs | FRN Financial | Bills & Fees" on the CORES Menu, then select FRN Financial and the view/make payments

[106] For questions regarding payment procedures, please contact the Financial Operations Group Help Desk by phone at 1-877-480-3201 (option #6).

[107] FCC Form 159 is accessible at https://www.fcc.gov/licensing-databases/fees/fcc-remittance-advice-form-159.

[108] Information completed using the Commission's Registration System (CORES) does not require the submission of an FCC Form 159. CORES is accessible at https://apps.fcc.gov/cores/userLogin.do.

[109] Instructions for completing the form may be obtained at http://www.fcc.gov/Forms/Form159/159.pdf.

option next to the FRN. Select the "Open Bills" tab and find the bill number associated with the NAL Acct. No. The bill number is the NAL Acct. No. with the first two digits excluded (e.g., NAL 1912345678 would be associated with FCC Bill Number 12345678). Finally, choose the "Pay from Bank Account" option. Please contact the appropriate financial institution to confirm the correct Routing Number and the correct account number from which payment will be made and verify with that financial institution that the designated account has authorization to accept ACH transactions.

33. Any request for making full payment over time under an installment plan should be sent to: Chief Financial Officer—Financial Operations, Federal Communications Commission, 45 L Street, NE, Washington, D.C. 20554.[110] Questions regarding payment procedures should be directed to the Financial Operations Group Help Desk by phone, 1-877-480-3201, or by e-mail, ARINQUIRIES@fcc.gov.

34. The written statement seeking reduction or cancellation of the proposed forfeiture, if any, must include a detailed factual statement supported by appropriate documentation and affidavits pursuant to sections 1.16 and 1.80(g)(3) of the Commission's rules.[111] The written statement must be mailed to the Office of the Secretary, Federal Communications Commission, 45 L Street, NE, Washington, D.C. 20554, ATTN: Enforcement Bureau – Telecommunications Consumers Division and must include the NAL/Account Number referenced in the caption. The statement must also be e-mailed to Daniel Stepanicich at Daniel.Stepanicich@fcc.gov.

35. The Commission will not consider reducing or canceling a forfeiture in response to a claim of inability to pay unless the petitioner submits the following documentation: (1) federal tax returns for the past three years; (2) financial statements for the past three years prepared according to generally accepted accounting practices; or (3) some other reliable and objective documentation that accurately reflects the petitioner's current financial status.[112] Any claim of inability to pay must specifically identify the basis for the claim by reference to the financial documentation. Inability to pay, however, is only one of several factors that the Commission will consider in determining the appropriate forfeiture, and we retain the discretion to decline reducing or canceling the forfeiture if other prongs of 47 U.S.C. § 503(b)(2)(E) support that result.[113]

[110] *See* 47 CFR § 1.1914.

[111] *Id.* §§ 1.16, 1.80(g)(3).

[112] 47 U.S.C. § 503(b)(2)(E).

[113] *See, e.g.*, *Ocean Adrian Hinson, Surry County, North Carolina,* Forfeiture Order, 34 FCC Rcd 7619, 7621, para. 9 & n.21 (2019); *Vearl Pennington and Michael Williamson*, Forfeiture Order, 34 FCC Rcd 770, paras. 18-21 (2019); *Fabrice Polynice, Harold Sido and Veronise Sido, North Miami, Florida*, Forfeiture Order, 33 FCC Rcd 6852, 6860-62, paras. 21-25 (2018); *Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc.*, Forfeiture Order, 33 FCC Rcd 4663, 4678-79, paras. 44-45 (2018); *Purple Communications, Inc.*, Forfeiture Order, 30 FCC Rcd 14892, 14903-04, paras. 32-33 (2015); *TV Max, Inc., et al*., Forfeiture Order, 29 FCC Rcd 8648, 8661, para. 25 (2014).

36. **IT IS FURTHER ORDERED** that a copy of this Notice of Apparent Liability for Forfeiture shall be sent by first class mail and certified mail, return receipt requested, to David Casem, CEO, Telnyx LLC, 311 West Superior St., Suite 504, Chicago, IL 60654 and Marc Martin, Perkins Coie LLP, 700 13th Street NW, Suite 800, Washington, DC 20005.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch

Secretary

DISSENTING STATEMENT OF COMMISSIONER NATHAN SIMINGTON

Re: *In the Matter of Telnyx, LLC*, File No.: EB-TCD-24-00037170, NAL/Acct. No.: 202432170009, FRN: 0018998724.

While the conduct described in this NAL is particularly egregious and certainly worth enforcement action, I continue to believe that the Supreme Court's decision in *Jarkesy* prevents me from voting, at this time, to approve this or any item purporting to impose a fine.

STATEMENT OF COMMISSIONER ANNA M. GOMEZ

Re: *In the Matter of Telnyx LLC*, EB File No. EB-TCD-24-00037170, Notice of Apparent Liability for Forfeiture (February 4, 2025)

It is important that service providers work quickly and closely with the FCC to identify and stop illegal traffic before it makes its way to consumers. I value self-reporting from industry actors on potential violations of our rules, and I am grateful the Office of Chairman Carr accepted our edits to this NAL to encourage self-reporting.