

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

In the Matter of)
Voxbeam Telecommunications Inc.)
File No.: EB-TCD-25-000386591
NAL/Acct. No.: 202632170002
FRN: 0019816354

NOTICE OF APPARENT LIABILITY FOR FORFEITURE

Adopted: March 31, 2026

Released: April 2, 2026

By the Commission:

I. INTRODUCTION

1. We propose a penalty of \$4,500,000 against Voxbeam Telecommunications Inc. (Voxbeam or Company) for apparently violating 47 CFR § 64.6305(g)(2) of the Federal Communications Commission’s (Commission or FCC) rules by apparently transmitting foreign traffic into the U.S. that used U.S. North American Numbering Plan (NANP) resources in the caller ID field, and which came from a foreign provider, Axfone, LLC (Axfone), not listed in the Robocall Mitigation Database (RMD). Between March 31, 2025 and April 3, 2025, Voxbeam transmitted tens of thousands of calls from Axfone onto the U.S. network. Many of the calls transmitted from Axfone through Voxbeam appear to spoof fraud prevention or customer services phone numbers belonging to U.S. financial institutions including Bank of America, Chase Bank, and others. Our rules related to the RMD are intended to promote transparency by ensuring that every provider in the database certifies they are taking measures to safeguard their networks from fraudulent traffic. The penalty we propose today is part of the Commission’s ongoing effort to hold providers accountable for failing to protect their networks from illegal robocallers.

II. BACKGROUND

2. Legal Framework. The Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act) required the Commission to mandate implementation of the STIR/SHAKEN caller ID authentication framework, which is designed to combat illegal caller ID spoofing, whereby bad actors falsify caller ID information to deceive call recipients into believing the caller is someone they trust, exposing consumers to fraudulent and malicious activity. Caller ID

1 The investigation began under File No. EB-TCD-25-00038193 and was subsequently assigned File No. EB-TCD-25-00038659. Any future correspondence with the Commission concerning this matter should reflect the new case number.

2 Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105 § 4(b), 133 Stat. 3274, 3277 (2019) (TRACED Act).

3 FCC Triennial Report on the Efficacy of the Technologies Used in the STIR/SHAKEN Caller ID Authentication Framework, Submitted to the Senate Committee on Commerce, Science and Transportation and House of

(continued....)

spoofing and fraud have resulted in significant losses to consumers. The Federal Bureau of Investigation (FBI) and Federal Trade Commission (FTC) both report that fraud, including spoofed calls, has caused billions of dollars in losses to consumers.⁴

3. Section 4(b)(5)(C)(i) of the TRACED Act further directed the Commission to require any voice service provider that had been granted a STIR/SHAKEN extension to implement “an appropriate robocall mitigation program to prevent unlawful robocalls from originating on the network of the provider.”⁵ The Commission adopted rules in October 2020 establishing the RMD and requiring voice service providers to file certifications in the RMD to promote transparency and effective robocall mitigation and to aid in monitoring compliance with robocall mitigation requirements.⁶ Voice service providers that certified to having implemented a robocall mitigation program were also required to file a robocall mitigation plan describing the reasonable steps they were taking to avoid originating illegal robocall traffic.⁷ These RMD certification requirements apply not only to domestic voice service providers but also to foreign voice service providers that use U.S. NANP numbers in the caller ID field to send voice traffic to residential and business subscribers in the United States.⁸ All voice service providers (including foreign voice service providers) were required to file certifications in the RMD by June 30, 2021.⁹ In May 2022, the Commission extended the requirement to file a certification in the RMD (including a robocall mitigation plan) to gateway providers, which are the first U.S.-based intermediate provider that receives a call directly from a foreign provider,¹⁰ and to foreign intermediate providers that use U.S. NANP numbers in the caller ID field to send voice traffic to the United States.¹¹ In March 2023, the Commission enhanced the information requirements for RMD filings and further expanded the requirement to file an RMD certification (including a robocall mitigation plan) to non-gateway

(Continued from previous page) _____

Representatives Committee on Energy and Commerce at 2 (2025) <https://docs.fcc.gov/public/attachments/DOC-416732A1.pdf>.

⁴ See Press Release, Fed. Trade Comm’n, New FTC Data Show a Big Jump in Reported Losses to Fraud to \$12.5 Billion in 2024 (March 10, 2025), <https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024> (consumers lost \$12.5 billion to fraud in 2024, with imposter scams accounting for \$2.95 billion). The FBI also reported that \$16.6 billion in scam and cybercrime losses in 2024, including losses due to spoofed calls. U.S. Dep’t of Justice, Fed. Bureau of Investigation, Internet Crime Report, at 10 (2024), https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

⁵ TRACED Act § 4(b)(5)(C)(i), codified at 47 U.S.C. § 227b(b)(5)(C)(i).

⁶ See *Call Authentication Trust Anchor*, WC Docket No.17-97, Second Report and Order, 36 FCC Rcd 1859, 1902-1903, paras. 82-83 (2020) (*Second Caller ID Authentication Order*). The relevant rules have evolved over time but are codified in 47 C.F.R. § 64.6305. As explained below, subsection (g)(2) of section 64.6305 is especially relevant to this NAL.

⁷ See *id.* at 1902, para. 82.

⁸ See *id.* at 1905, para. 90.

⁹ *Wireline Competition Bureau Announces Opening of Robocall Mitigation Database and Provides Filing Instructions and Deadlines*, WC Docket No. 17-97, Public Notice, 36 FCC Rcd 7394, 7394 (2021).

¹⁰ *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Sixth Report and Order, 37 FCC Rcd 6865, 6880, para. 34 (2022) (*Gateway Provider Report Order*). An “intermediate provider” is “any entity that carries or processes traffic that traverses or will traverse the public switched telephone network at any point insofar as that entity neither originates nor terminates that traffic.” 47 CFR § 64.6305(g)(2). A gateway provider is a “U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider. *Id.* § 64.6300(d); *Gateway Provider Order*, 37 FCC Rcd at 6876, para. 25.

¹¹ See *Gateway Provider Order*, 37 FCC Rcd at 6880, 6916, paras. 34, 128.

intermediate providers, so that now all domestic providers must file certifications (including a robocall mitigation plan) in the RMD.¹²

4. When the Commission adopted the RMD certification filing requirements for voice service providers in 2020, it also adopted a rule prohibiting U.S.-based intermediate providers and terminating voice service providers from accepting voice traffic directly from any voice service provider not listed in the RMD, including any foreign voice service provider that uses U.S. NANP numbers in the caller ID field to send voice traffic to residential or business subscribers in the United States.¹³ In May 2022, when the Commission extended RMD certification requirements to gateway providers and foreign intermediate providers, it extended the prohibition on U.S.-based providers accepting traffic directly from providers not listed in the RMD to include traffic received from gateway providers and foreign intermediate providers that are not listed in the RMD.¹⁴ With specific regard to accepting traffic from foreign providers, section 64.6305(g)(2) of our rules provides that:

[I]ntermediate providers and voice service providers shall accept calls directly from a foreign voice service provider or foreign intermediate provider that uses North American Numbering Plan resources that pertain to the United States in the caller ID field to send voice traffic to residential or business subscribers in the United States, only if that foreign provider's filing appears in the Robocall Mitigation Database . . . and that filing has not been de-listed pursuant to an enforcement action.¹⁵

North American Numbering Plan resources or NANP numbers “are ten-digit numbers consisting of a three-digit Numbering Plan Area (NPA) code, commonly called an area code, followed by a seven-digit local number.”¹⁶ “The format is usually represented as NXX-NXX-XXXX where N is any digit from 2 through 9 and X is any digit from 0 through 9.”¹⁷ NANP numbers specific to the United States include those reflecting an area code associated with a geographic region of the United States.¹⁸ While the Commission does not require foreign providers to file in the RMD, section 64.6305(g)(2) creates a strong incentive for foreign providers to do so if they wish to originate or transmit calls bearing a U.S. NANP number into the United States.¹⁹

5. *Factual Background.* Voxbeam certified as a voice service provider in its RMD filing and listed its primary business address in Orlando, Florida.²⁰ Voxbeam provides “wholesale service that

¹² See *Call Authentication Trust Anchor*, WC Docket No.17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573, 2592-93, paras. 37-38 (2023) (*Sixth Caller ID Authentication Order*) (expanding the requirements to all U.S.-based providers).

¹³ See *Second Caller ID Authentication Order*, 36 FCC Rcd at 1904, para. 86. In October 2021, the Commission temporarily stayed enforcement of the rule to the extent that it applied to voice traffic received directly from a foreign voice service provider that is not listed in the RMD. See *Gateway Provider Order*, 37 FCC Rcd at 6915-16, para. 126. In the *Gateway Provider Order*, the Commission lifted this stay and expanded the rule to also require blocking of traffic received directly from foreign *intermediate* providers, but delayed enforcement of the expanded rule until 90 days following the deadline for gateway providers to file certifications in the RMD. See *id.* at 6916, 6917, paras. 128, 131. Enforcement of the rule commenced on April 11, 2023. See 47 CFR § 64.6305(g)(2).

¹⁴ See *Gateway Provider Order*, 37 FCC Rcd at 6883-84, 6916, paras. 44, 128.

¹⁵ 47 CFR § 64.6305(g)(2).

¹⁶ NANPA, *About NANPA*, <https://www.nanpa.com/about> (last visited Mar. 6, 2026).

¹⁷ *Id.*

¹⁸ See NANPA, *Area Code Maps*, <https://www.nanpa.com/resources/area-code-maps> (last visited March 6, 2026).

¹⁹ See *Second Caller ID Authentication Order*, 36 FCC Rcd at 1905, para. 90.

²⁰ See Voxbeam Telecommunications Inc. (RMD0001514), Fed. Commc'ns Comm'n, Robocall Mitigation Database (filed Mar. 4, 2026)(Voxbeam RMD Certification);

(continued....)

provides low-cost calling solutions to service providers, fixed and mobile operators, calling card providers . . . around the world.”²¹ Voxbeam claims to offer service to “over 200 countries and 2,000 fixed and mobile networks,” including “[d]irect interconnects with over 500 of the leading mobile and fixed operators.”²² Voxbeam did not certify as a gateway provider in its RMD filing.

6. On July 8, 2024, {[]} (Financial Institution) filed a consumer complaint with the Commission stating that unknown entities were calling its banking customers with spoofed caller ID information making it appear that the calls came from the Financial Institution’s fraud reporting number contained on the back of the bank’s debit cards.²³ Some customers were deceived by the spoofed calls and were defrauded of funds.²⁴ The FCC’s Enforcement Bureau (Bureau) worked with the Industry Traceback Group (ITG) to trace the source of the calls. The ITG is the registered consortium selected by the Bureau to lead industry efforts to trace back suspected illegal robocalls to determine their origination.²⁵ At the Bureau’s request, the ITG conducted tracebacks and determined foreign provider Axfone as the source of one of the suspected illegal calls.²⁶

7. Axfone is a voice service provider located in Czechia.²⁷ Axfone claims that it provides services to “not only private households, small and medium-sized enterprises but also large international companies, government authorities and other public bodies.”²⁸ Axfone is not—and has never been—listed in the RMD.²⁹ During the Financial Institution’s investigation, a traceback response from Axfone listed the calling customer as “Tyler Perry.”³⁰ Axfone’s website shows a U.S. address in New York for an “Axfone USA” affiliate,³¹ but a physical FCC subpoena to Axfone at that address could not be served.

8. Four tracebacks sent by the ITG relating to calls on April 1 and April 2, 2025 identified Voxbeam as the gateway provider carrying suspected illegal spoofed impersonation robocalls directly

(Continued from previous page) _____
https://fccprod.servicenowservices.com/rmd?id=rmd_form&table=x_g_fmc_rmd_robocall_mitigation_database&sys_id=455b827d1b807c507ccf20ecac4bcb00&view=sp.

²¹ See Voxbeam, *About Us*, <https://www.voxbeam.com/about> (last visited Feb. 20, 2026).

²² See Voxbeam Home Page, <https://www.voxbeam.com/> (last visited Mar. 19, 2026).

²³ FCC Complaint #7143442 (July 8, 2024) (on file in EB-TCD-25-00038193).

²⁴ {[]}, Investigative Summary Report Re: Spoof calls from Florida fraud Group pretending to be Fraud Department at 1, 3-4 (July 10, 2024) (Investigative Summary Report) (on file in EB-TCD-25-00038193).

²⁵ *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 (2023).

²⁶ ITG Subpoena Response (Aug. 9, 2024), traceback 18974 (ITG August 2024 Subpoena Response) (on file in EB-TCD-25-00038193).

²⁷ See Axfone, *About Company*, <https://www.axfone.eu/about-us/about-company/> (last visited Mar. 19, 2026).

²⁸ *Id.*

²⁹ See Export of All Robocall Mitigation Database Filings (Mar. 14, 2025) (on file in EB-TCD-25-00038193) (showing Axfone’s name is not listed among any of the business names associated with any filings ever submitted to the Robocall Mitigation Database); Email from Erik Beith, Attorney Advisor, FCC to David Konuch, Attorney Advisor, FCC (Feb. 24, 2026, 11:02 a.m. E.S.T.) (“As of today [Feb. 24, 2026], there is still no record of any past or present RMD filing under the business name “Axfone LLC””) (on file in EB-TCD-25-00038659) (Axfone RMD Verification).

³⁰ ITG August 2024 Subpoena Response, *supra* note 26, traceback 18974 (on file in EB-TCD-25-00038193).

³¹ See Axfone, *Contacts*, <https://www.axfone.eu/about-us/contacts/> (last visited Mar. 19, 2026).

from Axfone onto the U.S. network, including two suspected illegal financial impersonation robocalls.³² Call detail records obtained from Voxbeam show that Voxbeam transmitted 60,873 calls to U.S. numbers bearing U.S. NANP caller IDs directly from Axfone between March 31, 2025 and April 2, 2025 from over 2,812 distinct caller IDs.³³ Much of this traffic came from caller IDs reflecting phone numbers belonging to large U.S. banks including Bank of America and Chase Bank, among others.³⁴

9. During EB's investigation, Voxbeam acknowledged that it had not taken any steps to determine whether Axfone was listed in the RMD before accepting voice traffic from it on March 31, 2025, and the succeeding days.³⁵ Voxbeam stated Axfone had been a customer since 2012 for provision of "[i]nbound [Direct Inward Dialing numbers] in multiple countries" and is "still an active customer" but had not placed any calls between November 17, 2018 and March 31, 2025.³⁶ Voxbeam apparently did not have a procedure to check whether upstream providers, even those that were inactive for years, were listed in the RMD before carrying their traffic.³⁷ Voxbeam blocked Axfone on April 3, 2025,³⁸ less than one day after receiving the first of the four traceback requests that led to the Bureau's subpoena.³⁹

10. Voxbeam supplemented its initial response on March 6, 2026.⁴⁰ Voxbeam explained that the incident "involved a 'burst' exploit of a historically dormant account (inactive since 2018)."⁴¹ The Company flagged the traffic and blocked the traffic from Axfone within 72 hours after the traffic began and less than 24 hours since it received the ITG traceback.⁴² Furthermore, it continued to block over

³² See Email from Jessica Thompson, ITG, to David Konuch, Attorney Advisor, FCC (May 19, 2025) responding to FCC Subpoena dated May 16, 2025. Ms. Thompson uploaded ITG's response via Box link on May 20, 2025 (ITG May 2025 Subpoena Response) (on file in EB-TCD-25-00038659). Tracebacks 24828, 24881, 24919, and 24920 identified Voxbeam as the point of entry (POE) into the U.S. for all four calls. For each of those calls, Voxbeam notified the ITG that Axfone was the upstream foreign provider from which it had received the call. Two of the calls were part of a robocalling campaign impersonating a financial institution; the other two were part of a robocalling campaign impersonating Verizon. See *id.* The Bureau sent a subpoena to Voxbeam on September 15, 2025 seeking call detail records and other information concerning traffic accepted from Axfone. See Email from David Konuch, Attorney Advisor, FCC to Steve Kay, CEO, Voxbeam (September 15, 2025 21:56 E.S.T.). Voxbeam responded on October 20, 2025. See Email from Steve Kay, CEO, Voxbeam, to David Konuch, Attorney Advisor, FCC (October 20, 2025 9:06 a.m. E.S.T) (on file in EB-TCD-25-00038659) (Voxbeam Subpoena Response) (confirming Axfone calls).

³³ See Declaration of Olayemi Olatunji, FCC Enforcement Bureau at para. 5 (Mar. 19, 2026) (on file in EB-TCD-25-00038193) (Olatunji Decl.); Voxbeam Subpoena Response to Request for Documents (RFD) No. 2 (Voxbeam Call Detail Records).

³⁴ Olatunji Decl., at para. 6 and Ex. B (BNA search results showing telephone numbers for Axfone calls assigned to Chase Bank and Bank of America, Navy Federal Credit Union and healthcare provider Kaiser Permanente).

³⁵ See Voxbeam Subpoena Response, *supra* note 32, at Response to Request for Information (RFI) No. 6.

³⁶ *Id.* at Responses to RFI Nos. 1.b, 6.

³⁷ Voxbeam stated that Axfone "had not been using our service to call any destination since 2018-11-17 therefore did not appear on any reports to request any information." See *id.* at Response to RFI No. 6.

³⁸ See *id.* at Response to RFI No. 7 ("[Axfone] was identified on the 3rd April 2025 having sent calls to +1 destinations between the period of 2025-03-31 & 2025-04-02 their access to +1 was blocked 2025-04-03 07:03:15 UTC").

³⁹ See ITG May 2025 Subpoena Response, *supra* note 32, traceback 24828 (showing that Voxbeam was notified by the ITG on April 2, 2025 at 19:14 UTC).

⁴⁰ E-mail from Steve Kay, CEO, Voxbeam, to David Konuch, Attorney Advisor, FCC (Mar. 6, 2026, 4:39 EST).

⁴¹ *Id.*

⁴² *Id.*

200,000 call attempts from Axfone.⁴³ Since the incident, Voxbeam claims that it “specifically monitor[s] for ‘dormant account reactivation’ to prevent a recurrence” and “automatically rejects calls from any source that does not have a valid RMD number and the correct signing of calls.”⁴⁴

11. The Bureau verified a subset of 2,250 of the 60,873 calls and determined each verified call used a U.S. NANP number in the caller ID field and each reached a U.S. business or residential subscriber.⁴⁵ Specifically, of the 2,812 unique caller IDs used in calls that Voxbeam accepted directly from Axfone, the Bureau selected caller IDs that an Internet search identified as associated with Chase Bank and Bank of America, and confirmed that the numbers were associated with the banks through a “billing name and address” (BNA) check.⁴⁶ The Bureau selected these calls based on Axfone’s history of transmitting bank impersonation calls,⁴⁷ and the low likelihood that major U.S. banks would have routed calls through Czechia-based Axfone.

III. DISCUSSION

A. Voxbeam Apparently Failed to Block Traffic from Axfone

12. The Commission’s rules require providers to implement critical safeguards against illegal robocalls, such as the STIR/SHAKEN caller identification framework in their IP networks and robocall mitigation programs,⁴⁸ and to respond to traceback requests.⁴⁹ These rules require providers to implement “an appropriate robocall mitigation program” that includes reasonable steps to avoid originating or carrying illegal robocall traffic on their networks⁵⁰ and a commitment to responding to ITG tracebacks fully and within 24 hours and to cooperate with investigations of illegal robocalls, thereby helping to identify and eliminate illegal robocalls.⁵¹ The Commission’s rules require providers to file certifications in the RMD acknowledging that all of the calls that they originate or carry are subject to an appropriate robocall mitigation program and describing the specific reasonable steps that they have taken to avoid originating or carrying illegal robocall traffic.⁵² In addition, the Commission’s rules prohibit domestic providers from accepting calls directly from any other domestic provider that is not listed in the RMD,

⁴³ *Id.*

⁴⁴ *Id.*

⁴⁵ See Verified Call Detail Records; Olatunji Decl. *supra* n.33, at paras. 5-10. The Verified Call Detail Records include the call detail records for the 2,250 calls spoofing J.P. Morgan Chase Bank and Bank of America, including the date/time of each call, the caller ID number, and the called number. Staff verified that each call used a U.S. NANP number in the caller ID field and reached a U.S. residential or business subscriber. Olatunji Decl. *supra* n.33, at paras. 5-10.

⁴⁶ Olatunji Decl., *supra* note 33, at paras. 5-7 & Exh. B.

⁴⁷ See *supra* notes 26 and 30.

⁴⁸ See 47 CFR §§ 64.6301, 64.6302, 64.6305(a)-(c).

⁴⁹ See *id.* § 64.1200(n)(1).

⁵⁰ *Id.* § 64.6305(a)-(c).

⁵¹ See 47 CFR § 64.6305(a)(1)-(2) (requiring that each “voice service provider shall implement an appropriate robocall mitigation program” that “shall include reasonable steps to avoid originating illegal robocall traffic . . . a commitment to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.”); see also *id.* § 64.6305(b)(1)-(2) (similar requirements for gateway providers regarding carrying illegal robocall traffic); *id.* § 64.6305(c)(1)-(2) (similar requirements for non-gateway intermediate providers regarding carrying illegal robocall traffic); 47 CFR § 64.1200(n)(1) (requirement for all providers to respond fully to traceback requests within 24 hours).

⁵² See *id.* § 64.6305(d)(1), (2)(ii) (voice service providers); *id.* § 64.6305(e)(1), (2)(ii) (gateway providers); *id.* § 64.6305(f)(1), (2)(ii) (non-gateway intermediate providers).

and from accepting calls directly from any foreign provider that is not listed in the RMD if its calls use NANP numbers in the caller ID field.⁵³ These measures protect consumers by ensuring providers have implemented robocall mitigation efforts.⁵⁴

13. Voxbeam apparently repeatedly violated section 64.6305(g)(2), which requires that “intermediate providers and voice service providers shall accept calls directly from a foreign voice service provider or foreign intermediate provider that uses North American Numbering Plan resources that pertain to the United States in the caller ID field to send voice traffic to residential or business subscribers in the United States, only if that foreign provider’s filing appears in the [RMD].”⁵⁵

14. Although Voxbeam certifies in the RMD that it is not a gateway provider, traceback and call details records show that it served as a gateway provider for traffic from Axfone between March 31 and April 2, 2025, as it received 60,873 calls directly from Axfone (a foreign provider) and transmitted the calls to providers in the United States for termination.⁵⁶ The Bureau verified that at least 2,250 of these calls used U.S. NANP resources in the caller ID field, *i.e.*, that they used U.S. area codes from the NANP numbering scheme.⁵⁷ The Bureau also verified that Voxbeam transmitted these calls to numbers assigned to residential or business subscribers in the United States.⁵⁸ Voxbeam accepted calls directly from Axfone despite Axfone not appearing in the RMD. Axfone has never been listed in the RMD.⁵⁹

15. Voxbeam apparently did not take any measures to determine whether upstream providers that were onboarded as customers prior to April 11, 2023, the effective date of section 64.6305(g)(2), had filed in the RMD.⁶⁰ This enabled Axfone to transmit calls onto the U.S. network that Voxbeam was obligated to block. Providers often maintain relationships with customers that predate the RMD, which the Commission established in 2020.⁶¹ The facts present here show the importance of section 64.6305(g) of our rules and the need for providers to check the RMD prior to accepting calls directly from an upstream provider, rather than assuming that existing customers have filed in the RMD. Providers should be on the lookout for customers like Axfone, a customer from prior to 2023 that may have appeared dormant to Voxbeam, that may suddenly begin sending large volumes of traffic. Voxbeam’s failure to check the RMD in this case enabled tens of thousands of spoofed and potentially illegal calls to reach U.S. telephone subscribers.

16. We conclude that Voxbeam apparently violated section 64.6305(g)(2) of our rules when it accepted 2,250 verified calls directly from Axfone, a foreign provider that did not appear in the RMD, that used U.S. NANP resources in the caller ID field and were delivered to U.S. subscribers.

B. Proposed Forfeiture

17. Section 503(b) of the Act authorizes the Commission to impose a forfeiture against any entity that “willfully or repeatedly fail[s] to comply with any of the provisions of [the Act] or of any rule,

⁵³ See *id.* § 64.6305(g).

⁵⁴ See *id.*; see also 47 CFR § 64.6305(g)(2).

⁵⁵ 47 CFR § 64.6305(g)(2).

⁵⁶ See ITG May 2025 Subpoena Response, *supra* note 32, tracebacks 24828, 24881, 24919, and 24920 (showing Voxbeam’s role as a gateway provider for those four calls); see also Voxbeam Call Detail Records, *supra* note 32.

⁵⁷ See Olatunji Decl., *supra* note 33, at paras. 7-10; see also NANPA, *About NANPA*, <https://www.nanpa.com/about> (last visited Mar. 6, 2026).

⁵⁸ See Olatunji Decl., *supra* note 33, at para. 9.

⁵⁹ See Axfone RMD Verification, *supra* note 29.

⁶⁰ See Voxbeam Subpoena Response, *supra* note 32, at Response to RFI No. 6.

⁶¹ *Second Caller ID Authentication Order*, 36 FCC Rcd at 1902-03, para. 82.

regulation, or order issued by the Commission[.]”⁶² Section 503(b)(2)(D) of the Act, as adjusted for inflation, authorizes us to assess a forfeiture against violators that are not common carriers of up to \$25,132 for each violation or each day of a continuing violation, up to a statutory maximum for any continuing violation of \$188,491 for any single act or failure to act.⁶³ The Commission determined in the *Sixth Caller ID Authentication Order* that all classes of providers should be treated the same for violations of the Commission’s robocall mandatory blocking rules and therefore established the maximum forfeiture amount that Section 503(b) and our rules permit us to impose on non-common carriers (currently \$25,132) as the maximum per-call forfeiture for all providers, regardless of common carrier status.⁶⁴ The Commission also adopted a base forfeiture amount of \$2,500 for each call that a provider fails to block in violation of the Commission’s mandatory block rules, which include section 64.6305(g).⁶⁵

18. In exercising our forfeiture authority under section 503, we must 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.”⁶⁶ In consideration of these statutory factors, the Commission has adopted upward and downward adjustment criteria for Section 503 forfeitures that we consider when determining the appropriate penalty in any given case.⁶⁷ Using these criteria, we may adjust the base forfeiture amount upward for violations that are, for example, egregious, intentional, or repeated, or that cause substantial harm or generate substantial economic gain for the violator; and we may adjust the base forfeiture downward if, for example, the violation is minor or the violator establishes an inability to pay.⁶⁸ We have discretion, however, to depart from these guidelines, taking into account the particular facts of each individual case.⁶⁹

⁶² 47 U.S.C. § 503(b)(1).

⁶³ See *id.* § 503(b)(2)(D); 47 CFR § 1.80(b)(10). See *Amendment of Section 1.80(b) of the Commission’s Rules, Adjustment of Civil Monetary Penalties to Reflect Inflation*, Order, 40 FCC Rcd 25 (2025); see also *Annual Adjustment of Civil Monetary Penalties to Reflect Inflation*, 90 Fed. Reg. 3710 (Jan. 15, 2025) (setting January 15, 2025 as the effective date for the increases).

⁶⁴ *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2602, para. 55; see 47 CFR § 1.80(b)(9).

⁶⁵ See *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2602, para. 55; see also *id.* at 2601, para. 54 & n.200; 47 CFR § 1.80(b)(11) tbl. 1.

⁶⁶ 47 U.S.C. § 503(b)(2)(E).

⁶⁷ 47 CFR § 1.80(b)(11), tbl. 3; *The Commission’s Forfeiture Policy Statement and Amendment of Section 1.80 of the Rules to Incorporate the Forfeiture Guidelines*, Report and Order, 12 FCC Rcd 17087, 17100-01, para. 27 (1997) (*Forfeiture Policy Statement*), *recons. denied*, Memorandum Opinion and Order, 15 FCC Rcd 303 (1999).

⁶⁸ 47 CFR § 1.80(b)(11), tbl. 3.

⁶⁹ See *Forfeiture Policy Statement*, 12 FCC Rcd at 17098–99, para. 22 (noting that “[a]lthough we have adopted the base forfeiture amounts as guidelines to provide a measure of predictability to the forfeiture process, we retain our discretion to depart from the guidelines and issue forfeitures on a case-by-case basis, under our general forfeiture authority contained in Section 503 of the Act”).

19. As has been the case in past robocall enforcement actions that have involved tens of thousands or more of apparently illegal calls, we apply the base forfeiture to a subset of calls that the Commission verified to be apparently in violation of our rules.⁷⁰ The reasons for doing so, rather than proposing a forfeiture based on the total number of apparently illegal calls, are pragmatic. *First*, there may be practical limitations to the Commission's ability to analyze every apparently illegal call (e.g., to determine whether it used NANP resources that pertain to the United States in the caller ID field and was transmitted to a residential or business subscriber in the United States) when the call volume is in the tens of thousands or higher.⁷¹ *Second*, in such large calling schemes, we find that applying a base forfeiture amount (with any applicable upward or downward adjustment) to a subset of verified calls results in a proposed forfeiture that achieves the dual goals of penalizing wrongful conduct and establishing a deterrent against future violations.⁷² Each case is unique, and we must use our discretion in proposing an appropriate penalty to meet the specific circumstances.

20. The Bureau reviewed a subset of 2,250 of the 60,873 calls that Voxbeam accepted directly from Axfone with NANP numbers that pertain to the United States in the caller ID field.⁷³ The Bureau verified that each of the 2,250 calls accepted by Voxbeam directly from Axfone used NANP resources pertaining to the United States in the caller ID field, and that Voxbeam transmitted each call to a residential or business subscriber in the United States.⁷⁴ We multiply the base forfeiture of \$2,500 by the subset of 2,250 verified calls to yield a total proposed forfeiture of \$5,625,000.

21. After reviewing the section 503(b)(2)(E) adjustment factors, we find reason to adjust downward the total proposed forfeiture to account for “other matters as justice may require.”⁷⁵ Voxbeam took prompt action to mitigate the traffic, successfully blocking Axfone’s traffic within 24 hours of receiving the first of the four ITG traceback requests.⁷⁶ It is critical that voice service providers respond quickly to tracebacks and take effective steps to mitigate illegal robocall traffic.⁷⁷ The steps that Voxbeam took after the illegal traffic began, however, do not absolve the Company of its failings with respect to our RMD rules. A substantial penalty is necessary to ensure compliance with these critical rules. We therefore propose a twenty percent downward adjustment to the penalty yielding an adjusted total proposed forfeiture amount of \$4,500,000.

IV. CONCLUSION

22. Requiring that providers only accept traffic from providers whose filings appear in the RMD is one of the Commission’s most important enforcement tools for protecting consumers from illegal robocall traffic and spoofed calls. Had Voxbeam checked the RMD prior to transmitting Axfone’s calls, it would have known to block Axfone and prevented 60,873 spoofed calls from reaching U.S. subscribers.

⁷⁰ See e.g., *Sumco Panama SA et al.*, Forfeiture Order, 38 FCC Rcd 7235, 7258, para. 57 (2023) (applying the base forfeiture to a subset of verified calls); *Scott Rhodes*, Forfeiture Order, 36 FCC Rcd 705, 728, para. 54 (2021) (same); *Rising Eagle Capital Group – Cayman*, Forfeiture Order, 36 FCC Rcd 6225, 6256-57, para. 59 (2021) (same).

⁷¹ See e.g., *Sumco Panama SA et al.*, Notice of Apparent Liability for Forfeiture, 37 FCC Rcd 15427, 15460, para. 77 (2022) (*Sumco Panama NAL*); *Gregory Robbins, Interstate Brokers of America LLC, National Health Agents LLC*, Notice of Apparent Liability for Forfeiture, 37 FCC Rcd 2591, 2602, para. 33 (2022) (*Robbins NAL*).

⁷² See e.g., *Sumco Panama NAL*, 37 FCC Rcd at 15460, para. 77; *Robbins NAL*, 37 FCC Rcd at 2602, para. 33.

⁷³ See Olatunji Decl. *supra* note 33, at paras. 3-9 (explaining how the calls were verified).

⁷⁴ *Id.* at paras. 7-10.

⁷⁵ 47 U.S.C. § 503(b)(2)(E).

⁷⁶ E-mail from Steve Kay, CEO, Voxbeam, to David Konuch, Attorney Advisor, FCC (Mar. 6, 2026, 4:39 EST).

⁷⁷ See 47 CFR §§ 64.1200(n)(1),(4)-(5).

23. We have determined that Voxbeam apparently repeatedly violated section 64.6305(g)(2) of the Commission's rules. As such, Voxbeam is apparently liable for a forfeiture of \$4,500,000.

V. ORDERING CLAUSES

24. 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, Voxbeam Telecommunications Inc. is hereby **NOTIFIED** of this **APPARENT LIABILITY FOR A FORFEITURE** in the amount of four million, five hundred thousand dollars (\$4,500,000) for repeated violations of section 64.6305(g)(2) of the Commission's rules, 47 CFR § 64.6305(g)(2).

25. **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, Voxbeam Telecommunications Inc. **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 31 below.

26. In order for Voxbeam Telecommunications Inc. to pay the proposed forfeiture, Voxbeam Telecommunication Inc. 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, Voxbeam Telecommunication Inc. 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:⁷⁸

27. 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 or printed CORES form⁷⁹ must be faxed to the Federal Communications Commission at 202-418-2843 or emailed 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).⁸⁰ For additional detail and wire transfer instructions, go to <https://www.fcc.gov/licensing-databases/fees/wire-transfer>.

28. 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.

⁷⁸ For questions regarding payment procedures, please contact the Financial Operations Group Help Desk by phone at 1-877-480-3201 (option #6).

⁷⁹ 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>.

⁸⁰ Instructions for completing the form may be obtained at <http://www.fcc.gov/Forms/Form159/159.pdf>.

29. 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 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.

30. 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. 20554.⁸¹ Questions regarding payment procedures should be directed to the Financial Operations Group Help Desk by phone, 1-877-480-3201, or by email, ARINQUIRIES@fcc.gov.

31. 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.⁸² 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 emailed to Daniel Stepanicich, Chief, Telecommunications Consumers Division, FCC Enforcement Bureau at Daniel.Stepanicich@fcc.gov with a copy to EnforcementBureauTCD@fcc.gov.

32. 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.⁸³ 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.⁸⁴

⁸¹ See 47 CFR § 1.1914.

⁸² *Id.* §§ 1.16, 1.80(g)(3).

⁸³ 47 U.S.C. § 503(b)(2)(E).

⁸⁴ See, e.g., *Ocean Adrian Hinson, Surry County, North Carolina*, Forfeiture Order, 34 FCC Rcd 7619, 7621, para. 9 & n.21 (2019); *Veal 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).

33. **IT IS FURTHER ORDERED** that a copy of this Notice of Apparent Liability for Forfeiture and the Verified Call Detail Records shall be sent by first class mail and certified mail, return receipt requested, to Steve Kay, Chief Executive Officer, Voxbeam Telecommunications Inc., 6314 Kingspointe Pkwy, Suite 1, Orlando, Florida, 32819, United States of America, and via email at steve@localphone.com.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary