

INFOBIP VOICE, INC. & AFFILIATES

Robocall Mitigation Program

Updated:

November 2024

February 2026

May 2026

Table of Contents

I.	Robocall Mitigation Program Introduction.....	3
A.	Company Summary	3
B.	Filing of RMP and Implementation of STIR/SHAKEN	3
II.	Robocall Mitigation Program	4
A.	Implementing Knowing Your Customer and Know Your Upstream Provider Protocols	5
B.	Requiring Contractual Provisions to Mitigate Illegal Robocalls.....	5
C.	Validating Customer’s Right to Use Telephone Numbers	6
D.	Adhering to Prerequisites Before Accepting Traffic from Other Providers	7
E.	Automatically Blocking Calls on Do-Not-Originate List.....	8
F.	Analyzing and Monitoring Network Traffic Routing Through Infobip Voice’s Network	8
G.	Third-Party Analytics Vendor	9
H.	Investigating Suspicious Calling Patterns	9
I.	Ensuring Foreign Providers Are Not Using Infobip Voice to Carry or Process High-Volume Illegal Traffic onto the U.S. Network	9
J.	Authenticating Voice Traffic	9
K.	Responding to Commission, Law Enforcement and ITG Traceback Requests ..	10
L.	Designating an Employee Responsible for Addressing Robocall Mitigation- Related Issues.....	10
M.	Updates to Infobip Voice’s RMD Submission and RMP	11
N.	Employee Training.....	11
O.	Principals and Parent Companies	11

I. Robocall Mitigation Program Introduction

Pursuant to the applicable orders and regulations of the Federal Communications Commission (“FCC” or “Commission”), the following Robocall Mitigation Program (“RMP”) details the policies and practices that Infobip Voice, Inc. (“Infobip Voice”) and its Affiliates¹ (both Infobip Voice and Affiliates are collectively referred to herein as, “Infobip Voice”) have established to prevent unlawful robocalls from originating on, terminating to, or routing through Infobip Voice’s voice networks where it is operating as a Voice Service Provider, Gateway Provider, or Intermediate Provider. Unless defined differently herein, capitalized terms used herein have the same definitions as set forth under 47 C.F.R. § 64.6300.

A. Company Summary

Infobip Voice, Inc. (formerly Peerless Network, Inc.) and its Affiliates are subsidiaries of Peerless Network Holdings, Inc., a Delaware corporation. Consistent with the FCC’s Robocall Mitigation Database (“RMD”) filing instructions,² the Affiliates of Infobip Voice are also covered under this RMP and Infobip Voice has submitted the information regarding its “Other [FCC Registration Numbers]” and “Other DBA Names” in the Robocall Mitigation Database.³ Exhibit A to this RMP also includes this information for all of Infobip Voice’s covered Affiliates.

Peerless Network Holdings, Inc. is an innovative and global VoIP provider focused on customized, scalable, and high-quality business communications that gives you better quality, rates, and control. The Infobip Voice portfolio delivers a robust suite of cutting-edge voice, UCaaS, SIP, Messaging, APIs, MS Teams integration, and other collaboration products and services. With its own nationwide voice network, Infobip Voice is trusted by enterprises, Fortune 500 companies, world-leading MVNOs and IXCs, and the nation’s largest CLECs.

Depending on the services being provided, Infobip Voice and its Affiliates may serve as Voice Service Providers, Intermediate Providers, and/or Gateway Providers.

B. Filing of RMP and Implementation of STIR/SHAKEN

Infobip Voice has fully implemented STIR/SHAKEN and on May 14, 2021, submitted its certification that all voice traffic that originates on its network is authenticated with STIR/SHAKEN consistent with 47 C.F.R. § 64.6301(a). In accordance with the RMD 12/2022 Filing Instructions, FCC Rule 47 C.F.R. § 64.6305(b) and because Infobip Voice is a “Combined Gateway and Voice Service Provider” under these instructions, Infobip Voice has certified that it has “fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it carries or processes are compliant

¹ See Exhibit A for a List of affiliates, collectively referred to as, “Affiliates”.

² See Robocall Mitigation Database External Filing Instructions, Version: December 2022 (“RMD 12/2022 Filing Instructions”), available at <https://www.fcc.gov/sites/default/files/rmd-instructions.pdf> (last visited December 8, 2022). See also Wireline Competition Bureau Announces Deadlines for Gateway Provider Robocall Mitigation Requirements and Additional Compliance Dates and Filing Instructions, WC Docket No 17-97, DA 22-1303 (rel. Dec. 12, 2022) (“Public Notice”).

³ RMD 12/2022 Filing Instructions at 8.

with FCC Rule, 47 C.F.R. § 64.6302(b).”⁴ In addition, Infobip Voice has uploaded this RMP into the RMD because it “details the specific reasonable steps it has taken to avoid carrying or processing illegal robocall traffic” and has included “a commitment to respond fully and 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 carry or process calls.”⁵

Consistent with its STIR/SHAKEN implementation, Infobip Voice assigns appropriate attestation levels to traffic routed through its network in accordance with applicable legal requirements and industry best practices, including ATIS-1000080 and ATIS-1000081.

II. Robocall Mitigation Program

This RMP applies to Infobip Voice’s calling platforms and provides information on Infobip Voice’s policies and procedures on the following topics that are discussed in turn below which “details the specific reasonable steps it has taken to avoid carrying or processing illegal robocall traffic”:

- A. Implementing Knowing Your Customer and Know Your Upstream Provider Protocols
- B. Requiring Contractual Provisions to Mitigate Illegal Robocalls
- C. Validating Customer’s Right to Use Telephone Numbers
- D. Adhering to Prerequisites Before Accepting Traffic from Other Providers
- E. Automatically Blocking Calls on a Do-Not-Originate List
- F. Analyzing and Monitoring Network Traffic Routing Through Infobip Voice’s Network
- G. Third-Party Analytics Provider
- H. Investigating Suspicious Calling Patterns
- I. Ensuring Foreign Providers Are Not Using Infobip Voice to Carry or Process High-Volume Illegal Traffic onto the U.S. Network
- J. Authenticating Voice Traffic
- K. Responding to Commission, Law Enforcement and ITG Traceback Requests
- L. Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues
- M. Updating Infobip Voice’s RMD Submission and RMP
- N. Training Employees
- O. Principals and Parent Companies

⁴ 47 C.F.R. § 64.6302(b) (stating that Intermediate Provider shall “[a]uthenticate caller identification information for all calls it receives for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call, except that the intermediate provider is excused from such duty to authenticate if it: (1) Cooperatively participates with the industry traceback consortium; and (2) Responds fully and in a timely manner to all traceback requests it receives from the Commission, law enforcement, and the industry traceback consortium regarding calls for which it acts as an intermediate provider.”)

⁵ RMD 12/2022 Filing Instructions at 12-13. See also 47 C.F.R. § 64.6305(d)(2)(ii) (even if a gateway provider is fully compliance with STIR/SHAKEN, it must file an RMP that sets forth “[t]he specific reasonable steps the gateway provider has taken to avoid carrying or processing illegal robocall traffic as part of its robocall mitigation program, including a description of how it has complied with the know-your-upstream provider requirement in § 64.1200(n)(4)”).

A. Implementing Knowing Your Customer and Know Your Upstream Provider Protocols

Consistent with the Wireline Competition Bureau’s Caller ID Authentication Best Practices No. 1⁶ and 47 C.F.R. § 64.1200(n)(3), Infobip Voice vets “the identity of retail and wholesale subscribers, in conjunction with (i) approving an application for service; (ii) provisioning of network connectivity; (iii) entering into a contract agreement; or (iv) granting the right-to-use telephone number resources.”⁷ In so doing, Infobip Voice takes “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.”⁸

Infobip Voice has implemented appropriate Know Your Customer (“KYC”) and Know Your Upstream Provider (“KYUP”) protocols when onboarding new or renewing commercial and wholesale customers and providers. As part of its KYC and KYUP protocols, Infobip Voice requires any commercial/wholesale customer and provider to provide sufficient information to ensure its legitimacy. Among other things, Infobip Voice generally requires its customers and providers to provide the full legal name of the company (and its parent company if applicable), state or county of incorporation, the physical address of its operations, the billing name and address (when different), and contact name and telephone number, federal tax ID (if it is a U.S. entity), and nature of the customer’s business. If the company is a Voice Service Provider, Foreign Voice Service Provider, Intermediate Provider, and/or Gateway Provider, Infobip Voice confirms, in accordance with currently effective FCC rules, that the company is listed in the FCC’s RMD and has not been delisted pursuant to an enforcement action before accepting traffic from such entities.⁹ Infobip Voice requires a traceback history covering the previous twelve months and sample traceback records.

Infobip Voice’s onboarding for its commercial/wholesale customers and providers also includes an application for service that can be used as a condition precedent to the initial establishment of service. The acceptance of an application or order for service by an applicant whose credit has not been duly established may be subject to the deposit, advance payment and/or refusal of service provisions described in Infobip Voice’s rates, terms and conditions. In addition, Infobip Voice reserves the right to examine the credit record or other available external sources of credit of any applicant or customer. Customers without an established credit rating or with a negative credit rating are required to have a deposit with Infobip Voice in an amount equivalent of up to two months of actual or estimated monthly charges.

B. Requiring Contractual Provisions to Mitigate Illegal Robocalls

Voice service customers of Infobip Voice are subject to robust terms and conditions that (1) obligate

⁶ Wireline Competition Bureau Issues Caller ID Authentication Best Practices, WC Docket Nos. 17-97 and 20-324, DA 20-1526, at Appendix A (rel. Dec. 22, 2020) (“FCC’s Caller ID Authentication Best Practices”), available at <https://docs.fcc.gov/public/attachments/DA-20-1526A1.pdf>.

⁷ *Id.*

⁸ 47 C.F.R. § 64.1200(n)(3).

⁹ See 47 C.F.R. § 64.6305(e)(1)-(3).

customers not to use Infobip Voice's services for unlawful purposes; and (2) preserve Infobip Voice's right to terminate customers for violations of the law, regulation, or industry practice. For its commercial/wholesale customers, Infobip Voice requires that they enter into a Master Service Agreement ("MSA") with Infobip Voice. Infobip Voice's standard MSA includes a termination clause for violations of federal, state, and local laws, rules, and regulations applicable to use of Infobip Voice's services or its equipment. Infobip Voice may suspend or terminate the MSA (and all services provided to a customer) immediately upon notice if a customer fails to cure any fraudulent or otherwise unlawful activity. Infobip Voice, at its sole option, may also terminate the MSA (and all services provided to a customer) immediately upon notice if a customer fails to remedy a material breach of the MSA within 30 days, or the customer commits a material breach which cannot be remedied. Illegal robocalls are treated as a material breach under the MSA. In addition, the MSA permits Infobip Voice, after reasonable notice, to cancel/suspend any service which is determined to be in violation of any applicable law or regulation, and also prohibits the customer from operating in a manner that would violate any applicable international, federal, state or local law or regulation (including telemarketing sales rules, invasion of privacy and obscenity).

Furthermore, the MSA requires customers to inform Infobip Voice before sending short duration traffic (i.e., calls of 6 second duration or less); prohibits customers from engaging in blasting activities (e.g., auto-dialers, mass calling, fax blasting, etc.) without prior written approval; and permits Infobip Voice to take curative action (e.g., suspension/cancellation) for customer violations. Infobip Voice also retains the right to immediately suspend or terminate service (with or without warning) for violations of its Acceptable User Policy ("AUP"), which prohibits among other things: unauthorized/illegal/fraudulent use of services; falsifying call/IP information to mask the originator or for impersonation purposes; transmission/distribution/retrieval/storage of information/data/material in violation of any applicable law or regulation; and attempts to breach system and network security measures (e.g., unauthorized access, unauthorized monitoring, interference, fraud/forgery, denial of service attacks, virus transmission). Termination of service is a nonexclusive remedy for breach under the MSA (as well as violations of the AUP) and does not limit Infobip Voice's right to seek additional remedies such as legal recourse to recover all costs involved in enforcement.

C. Validating Customer's Right to Use Telephone Numbers

Infobip Voice has processes and procedures in place to authenticate the proper use of telephone numbers associated with calls routed over the Infobip Voice's network and combat number spoofing. If required by applicable law or regulation, Infobip Voice requires its customers to fully implement STIR/SHAKEN on their own networks. In cases where a customer is unable to fully implement STIR/SHAKEN, where permitted by applicable law or regulation, Infobip Voice may assist them with signing their traffic to ensure traceability of calls across the PSTN and ensure all FCC requirements for transiting traffic to US telecommunications networks are fulfilled. In cases where Infobip Voice signs traffic on behalf of a customer network, the customer must agree to additional contractual terms governing their traffic, use of phone numbers and specific obligations to investigate and prevent any suspected robocalling or otherwise fraudulent traffic.

Infobip Voice's standard service order also contains language prohibiting the misuse of telephone numbers (i.e., DIDs). For instance, customers are required to allocate all DIDs used in call processing,

and errors associated with unallocated DIDs are considered to be a misuse of DIDs which are subject to monetary penalties. Infobip Voice may also, in its sole discretion, take other actions under Infobip Voice's standard Service Order to address misuse of DIDs (or if Infobip Voice discovers or reasonably suspects any abuse or unlawful activity), including: commercially reasonable action on offending numbers in order to minimize misuse; verbal, e-mail or written warning notifying the customer of the misuse and the corrective action that must be taken; suspension, with or without warning, all or part of a customer's service; and/or termination, with or without warning, all or part of customer's service and may terminate customer's agreement.

In addition, Infobip Voice's standard service order requires customers to cooperatively address unlawful use or misuse of DIDs in a timely manner.

Infobip Voice also has processes and systems in place to ensure that customer telephone number assignment is properly inventoried and tracked. Prior to accessing Infobip Voice's telephone number portal to order telephone numbers, a customer must establish an account profile, which is established after customer vetting is complete, contracts finalized, and network services (e.g., trunk groups) ordered. Only approved customers may access the telephone number portal, and each customer has a Infobip Voice administrator assigned to their account.

D. Adhering to Prerequisites Before Accepting Traffic from Other Providers

Accepting traffic from domestic Voice Service Providers. In accordance with 47 C.F.R. § 64.6305(e)(1), Infobip Voice only accepts calls directly from a domestic Voice Service Provider only if that Voice Service Provider's filing appears in the RMD and that filing has not been de-listed pursuant to an enforcement action.

Accepting traffic from Foreign Voice Service Providers Foreign Intermediate Providers. In accordance with 47 C.F.R. § 64.6305(e)(2), beginning April 11, 2023, Infobip Voice only 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 and that filing has not been de-listed pursuant to an enforcement action.

Accepting traffic from Gateway Providers. In accordance with 47 C.F.R. § 64.6305(e)(3), beginning April 11, 2023, Infobip Voice only accepts calls directly from a Gateway Provider only if that Gateway Provider's filing (a) appears in the RMD, (b) shows that the Gateway Provider has affirmatively submitted the filing, and (c) has not been de-listed pursuant to an enforcement action.

Public safety blocking safeguards. Despite the above paragraphs in this Section, in accordance with 47 C.F.R. § 64.6305(e)(4) and 47 C.F.R. § 64.1200(k)(5)-(6), Infobip Voice does not block a voice call if the call is an emergency call placed to 911. In addition, Infobip Voice makes all reasonable efforts to ensure that it does not block any calls from public safety answering points and government emergency numbers.

E. Automatically Blocking Calls on Do-Not-Originate List

In accordance with FCC Rules, 47 C.F.R. § 64.1200(k)(2), (n), and (o), Infobip Voice blocks any calls purporting to originate from a number on a reasonable Do-Not-Originate (“DNO”) list. This DNO only includes:

1. Numbers for which the subscriber to which the number is assigned has requested that calls purporting to originate from that number be blocked because the number is used for inbound calls only;
2. North American Numbering Plan (“NANP”) numbers that are not valid;
3. Valid NANP Numbers that are not allocated to a provider by the NANP Administrator; and
4. Valid NANP numbers that are allocated to a provider by the NANP Administrator, but are unused, so long as the provider blocking the calls is the allocate of the number and confirms that the number is unused or has obtained verification from the allocate that the number is unused at the time of blocking.

Infobip Voice adheres to the requirements outlined in 47 C.F.R. § 64.1200(k), which directs voice service providers to employ a “reasonable” Do-Not-Originate list as part of their robocall mitigation obligations, consistent with the FCC’s 2025 compliance deadline. In alignment with this mandate, Infobip Voice has invested in the Somos DNO solution and has fully integrated it into our call-processing systems to ensure comprehensive and up-to-date DNO coverage. Infobip Voice also incorporates DNO resources made available through the Industry Traceback Group (ITG), as appropriate, to further strengthen our ability to identify and block calls that purport to originate from numbers that should never generate outbound traffic.

F. Analyzing and Monitoring Network Traffic Routing Through Infobip Voice’s Network

Upon receiving call traffic, Infobip Voice also analyzes and monitors the call traffic that originates on, terminates to, or routes through Infobip Voice’s voice network. Consistent with Principle #5 of the FCC’s Caller ID Authentication Best Practices, Infobip Voice monitors the voice traffic patterns on a twenty-four (24) hour basis to identify behaviors that are consistent with illegal robocalling. If there are such calling patterns, Infobip Voice, after further investigation, takes appropriate action to address such behaviors, including terminating the customers service or blocking the calls.

As part of its analysis and monitoring of network traffic, Infobip Voice maintains a Network Operations Center (“NOC”) that provides continuous oversight of Infobip Voice’s voice service operations. Infobip Voice’s NOC staff is available 24-7-365 basis. The NOC is staffed by technicians and supervisors that have access to network engineering and vendor resource support, including additional support in the event of escalation incidents. Infobip Voice also maintains a team whose goal is to prevent fraudulent calls and abuse of Infobip Voice’s network; to detect and terminate such fraud should it occur; and to respond to fraud complaints, law enforcement inquiries and traceback requests. Infobip Voice uses specific email distribution lists (e.g., fraud@peerlessnetwork.com) to ensure that fraud matters are directed to the appropriate team members and handled in a timely manner.

G. Third-Party Analytics Vendor

Pursuant to 47 CFR § 64.6305(d)(2)(ii), (e)(2)(ii), and (f)(2)(ii), Infobip Voice is required to describe whether it uses any third-party analytics vendor(s) and the name(s) of such vendor(s). Infobip Voice, Inc. engages the services of a third-party analytics vendor; more specifically, Infobip Voice utilizes the services of TNS Call Guardian.

H. Investigating Suspicious Calling Patterns

When analyzing and monitoring call traffic, if Infobip Voice discovers call patterns that are consistent with illegal robocalling, Infobip Voice, after further investigation, takes appropriate action to address such behaviors and mitigate such traffic. These measures include, but are not limited to, working with the originating customer to resolve problematic traffic, termination of the subscriber originating such traffic, terminating the customer's service or blocking calls, as well as possible referrals to relevant enforcement agencies where appropriate. In the alternative, if the calls are determined to be legitimate, Infobip Voice will memorialize its findings in writing as needed.

I. Ensuring Foreign Providers Are Not Using Infobip Voice to Carry or Process High-Volume Illegal Traffic onto the U.S. Network

Pursuant to 47 C.F.R. § 64.1200(n)(4) and its January 16, 2023 effective date, when Infobip Voice serves as a Gateway Provider for voice traffic that is routing through its network, Infobip Voice takes reasonable and effective steps discussed under Sections 5 and 6, above, to ensure that any Foreign Voice Service Provider or foreign Intermediate Provider from which Infobip Voice directly receives traffic is not using Infobip Voice, as a Gateway Provider, to carry or process a high volume of illegal traffic onto the U.S. network.

J. Authenticating Voice Traffic

Pursuant to 47 C.F.R. § 64.6301(a), when operating as a Voice Service Provider, Infobip Voice does the following (1) to the extent technically feasible, authenticates and verifies originator identification information for all SIP calls that exclusively transit its own network; (2) to the extent technically feasible, authenticates originator identification information for all SIP calls it originates and that it will exchange with another Voice Service Provider or Intermediate Provider and, to the extent technically feasible, transmit that call with authenticated caller identification information to the next Voice Service Provider or Intermediate Provider in the call path; and (3) verifies originator identification information for all SIP calls it receives from another Voice Service Provider or Intermediate Provider which it will terminate and for which the caller identification information has been authenticated.¹⁰

Pursuant to 47 C.F.R. § 64.6302(b) and (c), when operating as a Gateway or Intermediate provider, Infobip Voice will, by no later than June 30, 2023, authenticate caller identification information for all calls it receives that use North American Numbering Plan resources that pertain to the United States in the caller ID field and for which the caller identification information has not been authenticated and

¹⁰ 47 C.F.R. § 64.6301(a).

which it will exchange with another provider as a SIP call.¹¹

K. Responding to Commission, Law Enforcement and ITG Traceback Requests

Infobip Voice is committed to ensuring that its network is not utilized for the origination, termination or routing of unwanted and illegal robocalls. In accordance with the FCC’s regulations 47 C.F.R. § 64.6305(b)(2) and 47 C.F.R. § 64.1200(n)(1)(ii), Infobip Voice will respond to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium (“ITG”) within 24 hours¹² and will cooperate with such entities in investigating and stopping any illegal robocallers that attempt to use Infobip Voice’s network to carry or process calls.

Infobip Voice will take the steps to effectively mitigate illegal traffic when it receives actual written notice of such traffic from the Commission through its Enforcement Bureau and will comply with the requirements of such notice and do so in accordance with the applicable FCC rules.¹³

Relatedly, in addition to responding to traceback requests within 24 hours, Infobip Voice has been a long-standing member of the ITG Traceback Group. Infobip Voice cooperates with all traceback requests, participates in quarterly scheduled ITG Member calls, fully complies with the ITG Policies and Procedures; and follows the Best Practices set forth in Appendix A: Provider Best Practices of ITG’s Policies and Procedures (Revised April 2022) (“ITG’s Best Practices”), available at <https://tracebacks.org/wp-content/uploads/2022/04/ITG-Policies-and-Procedures-Updated-Apr2022.pdf> at Appendix A. These Best Practices include (1) Dedicated Point of Contact; (2) Ongoing Coordination; (3) Prompt Response; (4) Vet the Identity of Customers; (5) Mitigate Traffic Source; (6) Analyze and Monitor Network Traffic; (7) Investigate and Mitigate Suspicious Calls and Calling Patterns; (8) Privacy of Call Traceback Information.¹⁴ To mitigate illegal robocalling, Infobip Voice’s RMP has, among other things, incorporated the applicable Best Practices herein.

L. Designating an Employee Responsible for Addressing Robocall Mitigation-Related Issues

To further ensure Infobip Voice’s network is not utilized for the origination, termination, or routing of unwanted and illegal robocalls, Infobip Voice provides the following name, title, department, business address, telephone number, and email address of the individual within Infobip Voice that leads Infobip Voice’s team that handles robocall mitigation-related issues as well as responds to traceback inquiries from the FCC, ITG, and law enforcement agencies:

Contact Name:	Virginia Bodyfelt
Contact Title:	Director, Regulatory Affairs

¹¹ 47 C.F.R. § 64.6302(b) and (c).

¹² This is 24-hour window applies within business days, per rule 47 C.F.R. § 64.1200(n)(1)(ii) and as clarified by the Commission. See FCC 22-37, at n.211

¹³ See 47 C.F.R. § 64.1200(n)(2), (3) & (5).

¹⁴ Capitalized terms in this paragraph that are associated with the ITG are defined in ITG’s Policies and Procedures (Revised April 2022).

Contact Address: 550 W. Van Buren Street, Suite 330
Contact City: Chicago
Contact State and Zip Code: Illinois, 60607
Contact Telephone Number: (312) 506-0933
Contact Email: VoiceRegulatory@infobip.com

M. Updates to Infobip Voice's RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(c)(5) & (d)(5), Infobip Voice will update its submission in the RMD within 10 business days of any change to the applicable information it must provide in the RMD, including its RMP.

N. Employee Training

Infobip Voice has implemented a training program that focuses on ensuring that personnel receive appropriate training on issues related to illegal robocalls. Each member of the Infobip Voice NOC Department and all personnel responsible for addressing fraud reports and/or traceback requests will receive a copy of this RMP for their review and records. Infobip Voice will also include this RMP in its package of policy documents and other relevant materials that are distributed to all employees on an annual basis. Employees are instructed to direct any questions about the RMP to the contact identified in Section 11 above. Through this approach, Infobip Voice will seek to ensure that each of its employees are aware of the contents of this RMP, thereby increasing its effectiveness. The Director of Regulatory Affairs conducts annual meetings with key internal teams - including Sales, Customer Support, and Back-Office Support - to review the Infobip Voice Robocall Mitigation Plan, the company's Know Your Customer (KYC) processes, and related procedures for identifying and addressing unwanted or illegal traffic. These sessions reinforce Infobip Voice's compliance obligations, ensure that personnel across operational and customer-facing functions understand their roles in preventing illegal robocalls, and promote consistent application of the company's mitigation policies.

O. Principals and Parent Companies

Pursuant to paragraph 46 of the Sixth Caller ID Authentication Report and Order (FCC 23-18 adopted on March 16, 2023), Infobip Voice is required to provide information regarding our principals, affiliates, subsidiaries, and parent companies. Infobip Voice, Inc. is owned by Peerless Network Holdings, Inc. Peerless Holdings does not provide telecommunications services but is a holding company that wholly owns Infobip Voice, Inc., which, together with its affiliates, provides competitive local exchange carrier services in 49 states and the District of Columbia. These affiliates are listed herein in Exhibit A.

In 2022, Infobip Inc. (formerly known as OpenMarket Inc.) acquired Peerless Network Holdings, Inc. The acquisition occurred through a merger of a special purpose subsidiary of OpenMarket with and into Peerless Network Holdings, with Peerless Network Holdings as the surviving entity. Peerless Network Holdings is directly wholly owned by Infobip Inc. and Infobip Voice, Inc. is indirectly

wholly-owned by Infobip Inc.

Infobip Inc., a Michigan corporation, does not offer domestic telecommunications services, is indirectly wholly owned by Infobip Limited, a United Kingdom entity, which, in turn, is wholly-owned by Infobip Holdings Limited (Infobip Holdings), a Cayman Islands entity. The following entity and individuals own Infobip Holdings: OEP IB MidCo L.P. (OEP IB MidCo) (15.55% equity and 33.33% voting, Cayman Islands citizenship); Silvio Kutić (49.66% equity and 16.67% voting, Croatian and Italian citizenship); Izabel Jelenić (21.28% equity and 16.67% voting, Croatian citizenship); and Roberto Kutić (12.52% equity and 16.67% voting, Croatian and Italian citizenship).

Exhibit A

Company Name	FRN (If assigned)	OCN
Infobip Voice, Inc.	0017253535	
Peerless Network of Alabama, LLC		143J
Peerless Network of Arizona, LLC		579F
Peerless Network of Arkansas, LLC		978J
Peerless Network of California, LLC		373F
Peerless Network of Colorado, LLC		278F
Peerless Network of Connecticut, LLC		539F
Peerless Network of Delaware, LLC		349F
Peerless Network of District of Columbia, LLC		275F
Peerless Network of Florida, LLC		902E
Peerless Network of Georgia, LLC		909E
Peerless Network of Illinois, LLC		063E
Peerless Network of Indiana, LLC		279F
Peerless Network of Idaho, LLC		
Peerless Network of Kansas, LLC		018H
Peerless Network of Kentucky, LLC		035H
Peerless Network of Louisiana, LLC		062H

Peerless Network of Maine, LLC		925H
Peerless Network of Maryland, LLC		568G
Peerless Network of Massachusetts, LLC		268F
Peerless Network of Michigan, LLC		933G
Peerless Network of Minnesota, LLC		107F
Peerless Network of Mississippi, LLC		926H
Peerless Network of Missouri, LLC		225F
Peerless Network of Montana, LLC		
Peerless Network of Nebraska, LLC		
Peerless Network of Nevada, LLC		408F
Peerless Network of New Hampshire, LLC		927H
Peerless Network of New Jersey, LLC		264F
Peerless Network of New Mexico, LLC		377H
Peerless Network of New York, LLC		155E
Peerless Network of North Carolina, LLC		350F
Peerless Network of North Dakota, LLC		460H
Peerless Network of Ohio, LLC		284F
Peerless Network of Oklahoma, LLC		384H
Peerless Network of Oregon, LLC		157F
Peerless Network of Pennsylvania, LLC		967E
Peerless Network of Rhode Island, LLC		631G

Peerless Network of South Carolina, LLC		098H
Peerless Network of South Dakota, LLC		152J
Peerless Network of Tennessee, LLC		276F
Peerless Network of Texas, LLC		177F
Peerless Network of Utah, LLC		526H
Peerless Network of Vermont, LLC		061H
Peerless Network of Virginia, LLC		275G
Peerless Network of Washington, LLC		159F
Peerless Network of West Virginia, LLC		928H
Peerless Network of Wisconsin, LLC		227F
Peerless Network of Wyoming, LLC		
Airus, Inc.	0009034182	476H, 018J, 060G, 019J, 124J, 645H, 947H, 486J, 579H, 910F, 930H, 423H, 931H, 932H, 477H, 691H, 428H, 948H, 020J, 459H, 933H, 588H, 478H, 534H, 589H, 066G, 082J, 949H, 083J, 695H, 935H, 039J, 438H, 507H, 188J, 580H, 950H, 951F, 021J, 665H, 040J, 936H, 581H
Airus of Arkansas, Inc.		578H
Airus of Florida, Inc.		484H
Airus of New York, Inc.		363H

Airus Virginia, Inc.		726H
WaveNation, LLC	0024187569	700J
Infobip, Inc.		