

ROBOCALL MITIGATION PROGRAM DESCRIPTION

Iberia Voz & Data SLU
Pursuant to 47 CFR § 64.6305
Date: June 06, 2026

I. COMPANY OVERVIEW

Iberia Voz & Data SLU (hereinafter "the Company") is a telecommunications operator duly incorporated and registered in Spain, providing Voice over IP (VoIP) services, international voice termination, and Direct Inward Dialing (DID) numbers from countries across multiple continents. The Company operates exclusively as a Business-to-Business (B2B) service provider, serving enterprise customers, resellers, and interconnection partners worldwide.

The Company's network is fully IP-based and its operations, infrastructure, and corporate headquarters are located outside the United States. Iberia Voz & Data SLU delivers international voice services to and from the U.S. telephone network solely through interconnection agreements with downstream carriers and resellers, without maintaining any physical facilities, equipment, or points of presence within the United States.

II. STIR/SHAKEN IMPLEMENTATION STATUS

Iberia Voz & Data SLU is a **foreign voice service provider** as defined under the Commission's rules. The Company does not maintain physical infrastructure within the United States, and therefore does not have direct access to Secure Telephone Identity (STI) certificates issued by FCC-authorized Certificate Authorities under the STIR/SHAKEN governance framework.

As a foreign-based operator, the Company lacks control over the network infrastructure elements necessary to implement the STIR/SHAKEN call authentication framework as required under 47 CFR § 64.6301 for domestic U.S. providers. Consequently, Iberia Voz y Data SLU is unable to sign originated calls with STIR/SHAKEN credentials governed by the FCC's certificate authority framework.

In lieu of STIR/SHAKEN implementation, and consistent with the Commission's rules applicable to foreign voice service providers, the Company hereby describes the specific reasonable steps it takes to prevent the origination of illegal robocall traffic, as detailed in Section III below.

III. ROBOCALL MITIGATION PROGRAM

Iberia Voz & Data SLU has implemented a comprehensive Robocall Mitigation Program designed to detect, prevent, and respond to illegal robocall traffic. The program encompasses the following elements:

A. Know Your Customer (KYC) — Customer Onboarding Procedures

The Company applies rigorous due diligence procedures before activating services for any customer. These measures include:

1. All prospective customers are required to provide complete business identification, including legal entity name, country of incorporation, business registration number, tax identification number, and the identity of principal beneficial owners or authorized representatives.
2. Customers must submit a detailed description of their intended use of the Company's services, including expected monthly call volumes, primary geographic origination and termination markets, and the nature of the traffic (e.g., enterprise voice, carrier interconnect, DID resale).
3. Prior to service activation, each customer must execute a Master Service Agreement (MSA) that explicitly prohibits the use of the Company's services for any unlawful purpose, including origination of illegal robocalls, caller ID spoofing, fraudulent telemarketing, or any other activity that violates applicable telecommunications laws and regulations.
4. The Company conducts review of publicly available regulatory databases, industry blacklists, and reputational records as part of the onboarding process to screen for known bad actors.
5. Customers are contractually obligated to maintain accurate and current account information with the Company and to notify the Company promptly of any material changes in their business operations, ownership, or intended use of services.
6. Activation of high-volume or wholesale traffic accounts is subject to enhanced review, including evaluation of projected traffic patterns and reference checks with existing industry contacts where appropriate.

B. Know Your Upstream Provider Procedures

The Company exercises due diligence in the selection and ongoing oversight of its upstream network interconnection partners:

1. All upstream providers are evaluated prior to establishing interconnection, including review of their regulatory standing, industry reputation, and their own compliance programs for robocall mitigation.
2. Interconnection agreements with all upstream providers contain explicit contractual provisions requiring compliance with applicable telecommunications laws and regulations, including FCC rules governing illegal robocalls and caller ID spoofing.
3. The Company monitors traffic received from upstream providers for signs of illegal robocall patterns and reserves the right to suspend or terminate interconnection in cases of non-compliance or repeated violations.
4. The Company maintains records of its upstream provider relationships sufficient to support traceback requests and regulatory inquiries.

C. Traffic Monitoring and Analytics

The Company employs the following technical and operational measures to monitor traffic and identify potentially illegal robocall activity:

1. Real-time monitoring of call volume, call origination patterns, and termination destinations using automated network management systems capable of detecting anomalous activity.
2. Threshold-based alerting systems configured to flag unusual spikes in call volume, high call attempt rates, abnormally short call durations, or other traffic characteristics associated with automated dialing or robocall campaigns.
3. Regular review of traffic analytics reports to identify patterns indicative of illegal robocall activity, including simultaneous high-volume dialing to sequential number ranges or known blocked number lists.
4. Immediate investigation protocols upon detection of suspicious traffic patterns, with authority to place accounts under observation, impose traffic restrictions, or suspend service pending investigation.
5. Maintenance of call detail records (CDRs) and related documentation sufficient to support traceback investigations and regulatory inquiries.

D. Response to Identified Illegal Traffic

Upon detection of illegal robocall traffic or receipt of a complaint or traceback request, the Company will take the following actions:

1. Immediately initiate an internal investigation of the reported traffic, reviewing relevant call records, customer account information, and network logs.
2. Take prompt corrective action commensurate with the findings, including suspension or termination of the responsible customer's service where the evidence warrants.
3. Cooperate fully with the Federal Communications Commission, law enforcement agencies, and the industry traceback consortium (USTelecom) in all traceback investigations and inquiries.
4. Provide all relevant records, documentation, and information requested in connection with traceback investigations within the timeframes set forth in Section IV of this document.
5. Where appropriate, file notifications with relevant regulatory authorities regarding confirmed instances of illegal robocall activity.

IV. TRACEBACK RESPONSE COMMITMENT

Iberia Voz & Data SLU hereby commits to respond **fully and within 24 hours** to all traceback requests received from the Federal Communications Commission, law enforcement agencies, and the industry traceback consortium (USTelecom), and to cooperate fully with such entities in investigating and stopping any illegal robocallers that use the Company's services to originate, carry, or process calls.

The Company's designated robocall mitigation point of contact (identified in Section V below) is responsible for receiving, acknowledging, and coordinating the Company's response to all such

requests.

V. ROBOCALL MITIGATION POINT OF CONTACT

The following individual has been designated as the Company's robocall mitigation point of contact for all matters related to this program:

Name:	Cristina Setraru
Title:	CEO
Department:	Legal
Business Address:	Iberia Voz & Data SLU Calle Benlliure, 2 La Nucia, Alicante 03530 Spain
Telephone:	+34 865 453 000
Email:	support@iberiatelecom.com

VI. DECLARATION

I, the undersigned officer of Iberia Voz & Data SLU, declare under penalty of perjury that I am authorized to make this certification on behalf of the Company, that I have examined the foregoing Robocall Mitigation Program Description, and that all statements contained herein are true, accurate, and complete to the best of my knowledge and belief.



Signature

Cristina Setraru

CEO

Iberia Voz & Data SLU

Date

June 06, 2026

This Robocall Mitigation Program Description is filed pursuant to 47 CFR § 64.6305 and in accordance with the FCC Robocall Mitigation Database filing instructions (December 2022). Fields marked in red are placeholders to be completed before submission.