



## **ROBOCALL MITIGATION PLAN**

### **NEWCALL COMUNICACIONES INTEGRALES S.L.U.**

#### **Robocall Mitigation Plan**

Prepared for FCC Robocall Mitigation Database Compliance.

Pursuant to 47 C.F.R. § 64.6305

**Entity:** Newcall Comunicaciones Integrales S.L.U.

**FRN:** 0038409397

**Country:** Spain.

**Date:** [May, 4th 2026]

#### **1. Introduction and Scope.**

Newcall Comunicaciones Integrales S.L.U. (“Newcall”) maintains this Robocall Mitigation Plan in accordance with applicable requirements established by the Federal Communications Commission (“FCC”), including 47 C.F.R. § 64.6305, relating to the FCC Robocall Mitigation Database (“RMD”).

Newcall is an international telecommunications service provider operating from Spain and providing communications services involving U.S.-bound voice traffic and international telecommunications interconnection services.

As required under FCC regulations, providers of telecommunications service provider operating from Spain and providing communications services involving U.S.-bound voice traffic and international telecommunications interconnection services.

As required under FCC regulations, providers transmitting voice traffic to the United States must either implement the STIR/SHAKEN caller ID authentication framework or maintain and certify an appropriate robocall mitigation program designed to prevent the origination, transmission, carrying, or processing of illegal robocall traffic.

At this time, Newcall has not implemented the STIR/SHAKEN authentication framework on any portion of its network and therefore relies on robocall mitigation program consistent with 47 C.F.R. § 64.6305.



This Robocall Mitigation Plan describes the policies, technical controls, compliance, procedures, customer verification measures, traffic monitoring practices, traceback cooperation commitments, and enforcement mechanisms implemented by Newcall to reduce the risk of illegal robocall traffic traversing its network.

Newcall is committed to cooperating with the FCC, law enforcement authorities, the Industry Traceback Group (“ITG”), upstream and downstream providers, and other authorized entities in connection with the prevention, investigation, mitigation, and enforcement of unlawful robocall activity.

This Plan is intended to support Newcall’s registration and ongoing compliance obligations within the FCC Robocall Mitigation Database framework and may be updated periodically to reflect operational, technical, or regulatory developments.

## **2. Company Identification and Regulatory Status.**

Newcall Comunicaciones Integrales S.L.U. (“Newcall”), is a telecommunications company organized and operating under the laws of Spain, with its principal place of business located at Avenida de Burgos 12B, 2ª Planta, Madrid, Spain.

Newcall provides international telecommunications and voice- related communications services involving U.S.. bound traffic and international interconnection activities.

For purposes of FCC regulatory compliance, Newcall has obtained a Federal Communications Commission Registration (“FRN”) under the FCC Commission Registration System (“CORES”):

- FRN: 0038409397

Newcall is registering in the FCC Robocall Mitigation Database (“RMD”) as a Voice Service Provider in connection with the transmission of voice traffic associated with U.S. telecommunications networks and services.

At the time of this filing, Newcall has not yet obtained an Operating Company Number (“OCN”). The company may update its FCC Robocall Mitigation Database filing in the future should an OCN be assigned or additional regulatory information become applicable.

Newcall currently relies on a robocall mitigation program pursuant to 47 C.F.R. § 64.6305 and has not implemented the STIR/SHAKEN authentication framework on any portion of its network.



The company maintains internal compliance, fraud prevention, customer verification, and traffic monitoring procedures intended to reduce the risk of unlawful robocall traffic and to support cooperation with traceback and regulatory enforcement processes where required.

### **3. Description of Services.**

Newcall provides international telecommunications and voice-related communications services involving the routing, transmission, interconnection, and delivery of voice traffic associated with domestic and international telecommunications networks.

The company operates as an international telecommunications infrastructure, including interconnected communications environments involving wholesale, carrier, enterprise, and business telecommunications services.

The company's network infrastructure is designed to support lawful telecommunications traffic and commercially legitimate communications services while maintaining operational control intended to reduce the risk of fraudulent, abusive, or unlawful robocall activity.

Newcall does not permit the use of its services for unlawful robocalling activities, fraudulent traffic generation, illegal caller ID spoofing, or any telecommunications activity prohibited under applicable FCC regulations, the Telephone Consumer Protection Act ("TCPA"), the Truth in Caller ID Act, or other applicable laws and regulatory requirements.

As part of its operations, Newcall maintains compliance procedures, customer onboarding controls, traffic monitoring mechanisms, and mitigation measures intended to identify and address suspicious traffic patterns or potentially unlawful use of its network.

The company may cooperate with upstream providers, downstream providers, telecommunications carriers, law enforcement authorities, the Industry Traceback Group ("ITG"), and other authorized entities in connection with traceback requests, fraud investigations, or mitigation-related activities involving voice traffic traversing its network.

### **4. STIR/SHAKEN Implementation Status.**

Newcall has not implemented the STIR/SHAKEN authentication framework or any portion of its network and currently relies on a robocall mitigation program consistent with the requirements established under 47 C.F.R. § 64.6305.

At this time, Newcall does not perform STIR/SHAKEN call authentication signing operations and does not certify full or partial implementation of the STIR/SHAKEN framework within its operational environment.



The company's current compliance approach is therefore based on the implementation of reasonable robocall mitigation measures designed to reduce the risk of unlawful robocall traffic traversing its network, including customer verification procedures, traffic monitoring mechanisms, anti-spoofing controls, traceback cooperation procedures, and fraud mitigation practices.

Newcall's network infrastructure may technically support the transmission of SIP signaling information and related call authentication headers within interconnected telecommunications environments where applicable. However, the company has not activated or deployed STIR/SHAKEN authentication functionality as part of its current services or operational configuration.

Accordingly, Newcall currently certifies pursuant to 47 C.F.R. § 64.6305(d)(1)(iii) that it has not implemented the STIR/SHAKEN authentication framework on any portion of its network and instead maintains a robocall mitigation program intended to comply with applicable FCC robocall mitigation obligations.

Newcall may periodically evaluate future regulatory, operational, or technical developments relating to STIR/SHAKEN implementation requirements and may update its practices or FCC filings accordingly if necessary.

## **5. Customer Onboarding and KYC Procedures.**

Newcall maintains customer onboarding, verification, and Know Your Customer ("KYC") procedures designed to reduce the risk of unlawful, fraudulent, abusive, or non-compliant traffic traversing its network.

Prior to activating services, Newcall performs reasonable verification measures intended to confirm the identity, legitimacy, and business purpose of prospective customers. These onboarding procedures are implemented as part of the company's broader robocall mitigation and fraud prevention framework.

As part of the onboarding and verification process, Newcall may request and review information and documentation including:

- Corporate identification and registration information;
- Tax identification or equivalent business registration data;
- Commercial contact information;
- Description of the customer's intended use of the services;
- Traffic profile information, including expected traffic volume, geographic destinations, and nature of the communications services to be used;
- Additional compliance-related information where considered reasonably necessary.



Customer applications and onboarding requests may be subject to internal review procedures intended to identify potential compliance, fraud, spoofing, or robocall-related risks prior to service activation.

Newcall may also conduct risk-based assessments taking into account factors such as:

- Customer type;
- Geographic location;
- Nature of the proposed telecommunications activity;
- Traffic characteristics;
- Potential fraud indicators;
- Regulatory or operational risk considerations.

Only customers that successfully complete applicable onboarding and verification procedures may be approved for activation of services.

As part of the customer onboarding process, Newcall may require customers to accept contractual obligations relating to:

- Compliance with applicable laws and telecommunications regulations;
- Prohibition of illegal robocalls and unlawful caller ID spoofing;
- Cooperation with fraud investigation, traceback requests, or regulatory inquiries;
- Proper and lawful use of telecommunications services and numbering resources.

Newcall reserves the right to reject, suspend, restrict, or terminate services where the company reasonably identifies elevated fraud risks, suspicious activity, inaccurate customer information, non-cooperation, or potential unlawful use of its network or services.

## **6. Contractual Requirements and Prohibited Uses.**

Newcall maintains contractual and compliance requirements intended to prevent the use of its services for unlawful, fraudulent, abusive, or non-compliant telecommunications activities.

Customers using Newcall's services are required to comply with all applicable laws, regulations, industry standards, and telecommunications compliance obligations, including those relating to illegal robocalls, caller ID spoofing, fraudulent traffic, and misuse of telecommunications networks or numbering resources.

As part of its commercial and compliance framework, Newcall may require customers to accept contractual provisions prohibiting, among other activities:

- The originating or transmission of illegal robocalls;
- Fraudulent telecommunications activity;



- Unlawful caller ID spoofing practices;
- Traffic intended to deceive, defraud, harass, or cause harm;
- Misuse of numbering resources or telecommunications infrastructure;
- Transmission of unlawful, abusive, or non-compliant traffic in violation of FCC regulations or other applicable laws.

Customers are also expected to cooperate with reasonable compliance inquiries, fraud investigations, traceback requests, or regulatory reviews relating to traffic transmitted through Newcall's network or services.

Newcall reserves the right to monitor compliance with contractual obligations and to take reasonable mitigation or enforcement measures where suspicious, abusive, fraudulent, or potentially unlawful activity is identified.

Such measures may include:

- Requests for additional information or clarification;
- Temporary suspension of services;
- Blocking or restriction of traffic;
- Enhanced compliance review procedures;
- Immediate termination of services or commercial relationships where necessary.

Failure by a customer to cooperate with compliance-related investigations, traceback procedures, or mitigation measures may constitute grounds for suspension or termination of services.

These contractual and operational controls form part of Newcall's broader robocall mitigation framework intended to reduce the risk of unlawful traffic traversing its telecommunications environment and to support compliance with applicable FCC robocall mitigation requirements.

## **7. Traffic Monitoring and Fraud Detection.**

Newcall maintains traffic monitoring, fraud detection, and network supervision procedures intended to identify, investigate, mitigate, and prevent potentially unlawful, fraudulent, abusive, or suspicious telecommunications traffic traversing its network.

As part of its robocall mitigation framework, Newcall applies reasonable operational and technical measures designed to detect traffic patterns commonly associated with illegal robocalls, spoofing, fraud, or other non-compliant telecommunications activity.

The company may utilize internal monitoring systems, network analytics, operational review procedures, and fraud detection mechanisms to identify suspicious traffic indicators, including but not limited to:



- Unusual traffic spikes or abnormal traffic volumes;
- High-volume calling activity over short periods of time;
- Sequential or patterned dialing behavior;
- Abnormally short call durations or anomalous Average Call Duration (“ACD”) metrics;
- Suspicious traffic destinations or routing patterns;
- Invalid, malformed, or inconsistent Caller ID (“CLI”) information;
- Potential spoofing indicators;
- Traffic characteristics inconsistent with the customer’s expected business profile or declared use case.

Newcall may perform validation and review procedures relating to caller identification information and traffic integrity controls where operationally applicable.

Traffic identified as potentially suspicious, fraudulent, abusive, or non-compliant may be subject to enhanced review and investigation by the company’s operational, compliance, or fraud management personnel.

Where appropriate, Newcall may request additional explanations, supporting documentation, or remediation measures from customers associated with suspicious traffic activity.

If Newcall reasonably determines that traffic may involve illegal robocalls, spoofing, fraud, abusive telecommunications activity, or other violations of applicable regulations or contractual obligations, the company may implement mitigation or enforcement measures including:

- Temporary traffic blocking;
- Traffic restrictions or filtering;
- Enhanced traffic monitoring;
- Suspension of services;
- Immediate termination of services or interconnections where necessary.

Newcall maintains internal procedures intended to support timely response and escalation processes in connection with suspected unlawful traffic or compliance-related incidents.

These traffic monitoring and fraud detection controls form part of Newcall’s broader robocall mitigation program intended to reduce the risk of unlawful traffic being originated, transmitted, carried, or processed through its network or services.

## **8. Traceback Cooperation and Complaint Handling.**

Newcall maintains procedures intended to support cooperation with traceback requests, fraud investigations, regulatory inquiries, and complaints relating to potentially unlawful, fraudulent, spoofed, abusive, or non-compliant telecommunications traffic.



As part of its robocall mitigation framework, Newcall is committed to cooperating in good faith with the Federal Communications Commission (“FCC”), law enforcement authorities, the Industry Traceback Group (“ITG”), telecommunications providers, and other authorized entities in connection with the investigation and mitigation of suspected illegal robocall activity.

Newcall maintains internal processes designed to facilitate the review, escalation, investigation, and handling of traceback requests or compliance-related inquiries involving traffic transmitted, routed, carried, or processed through its network or services.

Upon receipt of a traceback request, complaint, or regulatory inquiry, Newcall may undertake actions including:

- Identification and review of relevant traffic records or routing information;
- Internal investigation of the traffic or customer activity associated with the request;
- Communication with the relevant customer, upstream provider, downstream provider, or interconnection partner where appropriate;
- Assessment of potential spoofing indicators, fraudulent activity, or non-compliant traffic behavior;
- Implementation of mitigation, restriction, suspension, or enforcement measures where reasonably necessary.

Newcall is committed to responding to traceback requests within reasonable timeframes consistent with applicable FCC robocall mitigation obligations and operational capabilities.

The company may maintain designated compliance or operational personnel responsible for managing traceback-related communications, regulatory coordination, and compliance escalation procedures.

Where legally permissible and operationally appropriate, Newcall may cooperate with authorized investigative or enforcement efforts and may provide relevant information necessary to support the identification, mitigation, or prevention of unlawful robocall activity.

Newcall also maintains procedures intended to receive, review, and address complaints relating to suspected fraudulent traffic, spoofing, robocalls, or misuse of telecommunications services associated with its network environment.

All relevant investigations, reviews, mitigation actions, and compliance-related activities may be documented internally for operational, compliance, audit, and regulatory purposes.



## **9. Mitigation and Enforcement Measures.**

Newcall maintains mitigation and enforcement procedures intended to prevent, restrict, investigate, and address potentially unlawful, fraudulent, abusive, spoofed, or non-compliant telecommunications traffic traversing its network.

As part of its robocall mitigation framework, Newcall may implement operational, technical, contractual, and compliance-based measures where suspicious traffic activity, regulatory concerns, fraud indicators, or potential violations of applicable laws or contractual obligations are identified.

Mitigation actions may be initiated following:

- Traffic monitoring alerts;
- Fraud detection indicators;
- Customer complaints;
- Traceback requests;
- Regulatory inquiries;
- Operational reviews;
- Reports from upstream or downstream providers;
- Internal compliance assessments.

Where appropriate, Newcall may undertake one or more mitigation or enforcement actions, including:

- Enhanced monitoring of traffic or customer activity;
- Requests for additional customer information or clarification;
- Investigation of suspicious traffic patterns or calling behavior;
- Temporary traffic restrictions or filtering measures;
- Blocking of suspicious or non-compliant traffic;
- Temporary suspension of services;
- Restriction of network access or interconnection capabilities;
- Escalation to internal compliance or management personnel;
- Termination of services, commercial relationships, or interconnection arrangements where necessary.

Newcall reserves the right to take immediate action where the company reasonably believes that traffic may involve:

- Illegal robocalls;
- Fraudulent telecommunications activity;
- Unlawful caller ID spoofing;
- Scam-related activity;
- Abuse of telecommunications infrastructure or numbering resources;



- Material violations of contractual or regulatory obligations.

Customers, partners, or interconnection counterparties may be required to cooperate with compliance investigations, traceback procedures, remediation efforts, or mitigation-related requests as part of Newcall's operational and regulatory compliance processes.

Failure to cooperate with reasonable compliance or mitigation measures may result in additional restrictions, suspension, or termination of services.

Newcall may also coordinate with upstream providers, downstream providers, telecommunications carriers, law enforcement authorities, the Industry Traceback Group ("ITG"), and other authorized entities where reasonably necessary to support the mitigation, prevention, investigation, or enforcement of unlawful telecommunications activity.

All mitigation-related investigations, enforcement actions, and compliance responses may be internally documented and retained for operational, audit, compliance, or regulatory purposes.

#### **10. Upstream and Downstream Provider Controls.**

Newcall maintains reasonable operational and compliance controls relating to upstream providers, downstream providers, interconnection partners, carriers, resellers, and other telecommunications entities interacting with its network or services.

As part of its robocall mitigation framework, Newcall may perform risk-based assessments and compliance reviews relating to interconnection relationships and telecommunications traffic sources associated with its operational environment.

Where operationally appropriate, Newcall may require telecommunications partners, customers, resellers, carriers, or service providers to comply with applicable telecommunications laws, regulatory obligations, anti-fraud requirements, and robocall mitigation standards.

Newcall may also request or verify information relating to:

- Regulatory registrations;
- Service legitimacy;
- Telecommunications licensing status;
- Traffic profiles;
- Nature of services provided;
- Compliance with applicable robocall mitigation obligations;
- Cooperation with traceback procedures and fraud investigations.



The company may evaluate upstream and downstream traffic relationships for indicators of suspicious, abusive, fraudulent, spoofed, or non-compliant traffic activity.

Traffic or interconnection relationships identified as presenting elevated operational, fraud, compliance, or regulatory risks may be subject to:

- Enhanced monitoring;
- Additional compliance review procedures;
- Traffic restrictions;
- Temporary suspension measures;
- Blocking actions;
- Termination of interconnection or commercial relationships where necessary.

Newcall may also cooperate with telecommunications providers, carriers, regulators, industry groups, and authorized entities in connection with traceback requests, fraud prevention efforts, robocall mitigation initiatives, and investigations relating to unlawful telecommunications activity.

The company seeks to maintain commercially reasonable controls intended to reduce the risk of illegal robocall traffic entering, traversing, or exiting its network through upstream or downstream telecommunications relationships.

These interconnection and provider oversight measures form part of Newcall's broader robocall mitigation and network integrity framework intended to support compliance with applicable FCC robocall mitigation requirements.

## **11. Governance, Review, and Recordkeeping.**

Newcall maintains internal governance, compliance oversight, and recordkeeping procedures intended to support the effectiveness, maintenance, and periodic review of its robocall mitigation framework.

The company may periodically review and update its robocall mitigation policies, operational controls, monitoring practices, and compliance procedures in response to:

- Regulatory developments;
- FCC guidance or enforcement trends;
- Emerging fraud risks or robocall threats;
- Operational or technical changes;
- Industry best practices;
- Internal compliance assessments or investigations.



Newcall's compliance, operational, management, or authorized personnel may participate in the review and oversight of mitigation-related procedures and network integrity controls where appropriate.

The company may also maintain internal procedures intended to support:

- Compliance escalation and reporting;
- Internal investigation processes;
- Operational risk management;
- Fraud prevention oversight;
- Regulatory coordination activities;
- Periodic assessment of mitigation effectiveness.

As part of its operational and compliance framework, Newcall may retain records, logs, documentation, and information relating to:

- Customer onboarding and verification activities;
- Traffic monitoring reviews;
- Fraud investigations;
- Traceback requests;
- Compliance inquiries;
- Mitigation actions;
- Suspension or enforcement measures;
- Regulatory communications;
- Internal compliance assessments.

Such information may be retained for operational, compliance, audit, legal, security, fraud prevention, or regulatory purposes, subject to applicable legal and data protection requirements.

Newcall may also maintain internal documentation relating to policy updates, procedural revisions, operational changes, and mitigation-related governance decisions in order to support accountability, auditability, and ongoing compliance efforts.

This Robocall Mitigation Plan may be updated periodically to reflect material operational, regulatory, technical, or compliance-related developments affecting the company's telecommunications services or mitigation obligations.



## **12. Conclusion and Compliance Commitment**

Newcall is committed to maintaining and enforcing reasonable robocall mitigation measures designed to reduce the risk of unlawful, fraudulent, abusive, spoofed, or otherwise non-compliant telecommunications traffic traversing its network or services.

Through the implementation of customer onboarding controls, Know Your Customer (“KYC”) procedures, contractual compliance requirements, traffic monitoring mechanisms, fraud detection processes, traceback cooperation procedures, and mitigation and enforcement measures, Newcall seeks to support the integrity, security, and lawful operation of its telecommunications environment.

The company is committed to cooperating in good faith with the Federal Communications Commission (“FCC”), law enforcement authorities, the Industry Traceback Group (“ITG”), telecommunications providers, and other authorized entities in connection with the prevention, investigation, mitigation, and enforcement of unlawful robocall activity.

Newcall currently maintains a robocall mitigation program pursuant to 47 C.F.R. § 64.6305 and has not implemented the STIR/SHAKEN authentication framework on any portion of its network at this time.

The company may periodically review and update its operational practices, mitigation controls, compliance procedures, and regulatory filings as necessary to address evolving operational, technical, fraud-related, or regulatory developments.

By maintaining this Robocall Mitigation Plan and related compliance procedures, Newcall seeks to promote responsible telecommunications practices, support regulatory compliance obligations, and contribute to broader industry efforts aimed at combating illegal robocalls, spoofing, fraud, and misuse of telecommunications networks.