

Robocall Mitigation Plan

1. Introduction

As a provider that routes voice traffic to the United States, we maintain a Robocall Mitigation Plan consistent with Federal Communications Commission (FCC) requirements and have submitted the corresponding certification to the FCC's Robocall Mitigation Database (RMD).

Under FCC rules (47 CFR § 64.6305), all voice service providers in the call path to or within the U.S. must either implement STIR/SHAKEN caller ID authentication or maintain and certify a robocall mitigation program that includes:

- Reasonable steps to prevent the origination of illegal robocall traffic,
- A commitment to full cooperation with law enforcement and traceback requests.

As a non-U.S.-based provider not eligible to obtain STIR/SHAKEN credentials under the U.S. framework, we have implemented a mitigation-based compliance program consistent with FCC requirements and have certified our practices in the RMD, covering all U.S.-bound traffic transiting our network.

2. Contractual Requirements and Prohibitions

All customer agreements strictly prohibit the origination of unlawful robocalls, as defined under the U.S. Telephone Consumer Protection Act (TCPA), the Truth in Caller ID Act, and relevant FCC regulations (e.g., 47 CFR § 64.1200, § 64.6305). Customers must not transmit any traffic that violates these laws or engage in practices such as caller ID spoofing with the intent to defraud, cause harm, or wrongfully obtain anything of value.

Our Outbound Service Order—executed prior to service activation—includes explicit compliance obligations. These include:

- Mandatory adherence to this Robocall Mitigation Plan;
- A prohibition on abusive call patterns, spam, or unlawful spoofing;
- An obligation to fully cooperate in any investigation concerning their traffic;
- Commitment to maintain traffic characteristics consistent with legitimate usage.

Traffic monitoring includes the evaluation of key metrics such as minimum Answer-Seizure Ratio (ASR) and Average Call Duration (ACD), which are defined in the Outbound Service Application Form. Deviation from expected thresholds may trigger enhanced review, suspension, or termination of services.

Enforcement Clause

Clause 5.2.7. The Customer shall co-operate with DIDWW in relation to any complaints, enquiries or investigations regarding services offered by the Customer. The Customer shall, at the discretion of DIDWW, without limitation bear in full any costs associated with such complaints, investigations, or enquiries or any action whether brought by DIDWW or brought against DIDWW.

3. Customer Onboarding and KYC Verification

We maintain a robust customer onboarding and Know Your Customer (KYC) process as a critical control in our Robocall Mitigation Program. No outbound calling services are activated until the prospective customer successfully completes all verification steps and formally accepts our compliance obligations.

As part of this onboarding process:

- All new customers must submit a completed Outbound Service Application Form, which includes:
 - Business verification documentation, such as a certificate of incorporation, tax identification number, and company profile or business license;
 - A detailed traffic profile, including the nature and intended purpose of the calls, estimated call volumes, primary destination types, and the categories of end-users served;
 - A certification of compliance with applicable laws and regulations, including FCC robocall mitigation rules.
- Each application is subject to a comprehensive review by our internal compliance team. This includes:
 - Validation of business identity and operational legitimacy;
 - Review of traffic use cases to confirm they align with lawful and permitted service categories;
 - Risk screening based on customer type, geography, and service model.
- Only upon successful completion of this review is the customer approved for service. At that point, the customer must sign our Outbound Service Order and/or Agreement, which explicitly acknowledges:
 - Prohibition of illegal robocall activity and caller ID spoofing practices;
 - Mandatory compliance with this Robocall Mitigation Plan;
 - Obligation to cooperate with all investigations, complaint inquiries, and traceback requests initiated by regulatory bodies or our internal compliance function.

Outbound calling capabilities are enabled only after the signed Outbound Service Order is received and all onboarding checks are complete. This end-to-end vetting process ensures that only legitimate, compliant customers gain access to our outbound voice services, thereby reducing the risk of unlawful traffic originating through our network.

4. Traffic Monitoring and Traceback Response

We maintain a continuous traffic monitoring program designed to detect and respond to unlawful or suspicious call behaviour. Our network operations and compliance teams utilize real-time analytics and automated alerting systems to flag indicators of potentially illegal robocall activity, including:

- Unusually short call durations or low average call durations;
- High volumes of calls over short periods;
- Sequential or patterned dialing behaviors;
- Invalid or malformed Caller ID (CLI) formats inconsistent with national or international numbering plans.

All outbound calls are subject to CLI validation to detect non-compliant caller identities. Caller ID (CLI) values are automatically validated against E.164 formatting and length requirements. Traffic with invalid or anomalous CLI formats is rejected and escalated for customer explanation.

When suspicious activity is identified, our compliance team immediately initiates an investigation. The customer is formally contacted and required to justify or verify the legitimacy of the flagged traffic. Failure to provide a satisfactory explanation or remediation may result in immediate suspension or termination of service.

We are an active participant in the Industry Traceback Group (ITG), as recognized by the FCC, and respond to all traceback requests in accordance with 47 CFR § 64.1200(n)(2). In the event of a traceback request from the FCC, the Industry Traceback Group (ITG), or other authorized enforcement entities, we are committed to responding within 24 hours, as mandated by the FCC. Upon receipt of such a request, we:

- Identify the source of the call within our network;
- Notify the relevant customer and request a detailed response regarding the traffic in question;
- Enforce immediate corrective action where a violation is confirmed.

A designated internal compliance team serves as the single point of contact for handling all traceback-related matters. We fully cooperate with all legitimate investigative efforts and, in accordance with applicable laws and data protection obligations, may share relevant information to aid in the identification and mitigation of illegal robocall sources. All investigations and actions taken are logged to ensure full auditability and regulatory defensibility.

This integrated approach—combining automated traffic surveillance with a rapid, structured traceback response—ensures our network complies with FCC rules and maintains a strong defensive posture against illegal robocall origination.

Customer traffic is subject to ongoing monitoring post-activation. Accounts may be flagged for enhanced scrutiny based on risk indicators such as unusual traffic bursts, new destinations, or complaints. Mitigation controls may include alerts, or temporary suspension pending review.

5. Robocall Mitigation Database Compliance and Partner Enforcement

We maintain an active and up-to-date registration in the FCC RMD, as required under 47 CFR § 64.6305. Under FCC rules, U.S.-based voice service providers are prohibited from accepting voice traffic directly from any upstream or intermediate provider not listed in the RMD, including foreign voice service providers that originate or deliver U.S.-bound traffic.

While we are not a U.S.-based provider, we apply equivalent compliance controls to align with these requirements and ensure accountability throughout the call path. Specifically:

- Our company's RMD certification is actively maintained and reflects our current robocall mitigation practices.
- All wholesale customers (including international carriers and resellers) must provide documented proof of their RMD registration before activating service for U.S.-bound traffic. This is a mandatory precondition for provisioning.
- Any provider that fails to maintain active RMD registration is subject to immediate traffic suspension and potential service termination.
- We only accept inbound traffic from upstream interconnect partners if they are currently listed in the RMD and subject to FCC-recognized mitigation obligations.

By enforcing RMD compliance throughout our customer and interconnect ecosystem, we uphold call path accountability and reduce the risk of unlawful robocall traffic traversing our network. This approach supports the integrity of the U.S. telephone system and aligns our operations with FCC-mandated mitigation standards.

6. Customer Awareness and Policy Governance

As part of our robocall mitigation framework, we maintain a structured approach to internal training, customer awareness, and ongoing policy maintenance to ensure continuous alignment with evolving regulatory obligations and industry best practices.

6.1. Internal Staff Enablement

- Our sales, compliance, and account management teams receive regular training and guidance on robocall mitigation requirements, including:
 - FCC restrictions on auto-dialed or prerecorded voice calls to U.S. numbers without prior express consent, as governed by the Telephone Consumer Protection Act (TCPA) and FCC 47 CFR § 64.1200;
 - Indicators of high-risk use cases and red flags to identify potentially unlawful traffic;
 - Procedures for escalating customer inquiries or compliance concerns to the internal compliance team.

6.2. Ongoing Policy Review and Updates

- This Robocall Mitigation Plan is reviewed at least annually or sooner if required by:
 - New or updated FCC rules or enforcement guidance;
 - Emerging robocall threats, technologies, or industry mitigation standards.
- Revisions to this policy are subject to internal approval by our compliance and legal functions. Version control and change history are maintained as part of our policy documentation lifecycle.

6.3. Customer Communication and Policy Awareness

- Educational materials and updated usage guidelines are shared with customers to support ongoing compliance and risk mitigation.

Through this combination of internal education, policy governance, and external communication, we promote a shared understanding of legal and technical obligations, reduce the risk of inadvertent violations, and strengthen the overall resilience of our voice traffic ecosystem.

7. Corporate Ownership and Affiliations

We certify that we are a standalone legal entity with no parent company. We maintain no affiliated voice service entities subject to robocall mitigation obligations under FCC rules. We have no previous business names or additional DBAs. Information regarding our management control has been submitted via the RMD certification form.

8. Conclusion

This Robocall Mitigation Plan outlines our company's formal commitment to preventing the origination of unlawful robocall traffic and maintaining full compliance with applicable U.S. FCC regulations. We implement a multi-faceted mitigation strategy that includes:

- Rigorous customer onboarding and Know Your Customer (KYC) procedures;
- Binding contractual prohibitions against illegal robocalling and spoofing;
- Real-time traffic monitoring, anomaly detection, and caller ID validation;
- Full cooperation with traceback efforts initiated by the FCC, Industry Traceback Group (ITG), or authorized enforcement bodies;
- Immediate enforcement actions, including blocking or suspension of traffic deemed unlawful or non-compliant.

We are committed to the ongoing execution, periodic review, and continuous improvement of this Plan in response to evolving threats and regulatory developments. Our compliance team maintains accountability for implementation and regulatory communication.

By adhering to this framework, we protect the integrity of our network, uphold our responsibilities as an international voice service provider, and contribute to the global effort to combat illegal robocalls. Our active registration in the FCC's RMD affirms our good standing and operational commitment to lawful voice traffic delivery.