

ROBOCALL MITIGATION PLAN (RMP)

Pursuant to 47 C.F.R. § 64.6305, Advanced Cloud Services SL hereinafter “ACS” submit this plan to prevent and mitigate illegal robocalls, as of February 26 2024. ACS reserves the right to modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time as it deems appropriate to reflect its business, its capabilities, its needs and FCC obligations.

STIR/SHAKEN

ACS has been in the telecommunications business since 2021 and is a global service provider offering a complete range of voice and messaging services - designed to meet the fast-changing needs of national and international Carriers, OTTs, ISPs, Media/Content Providers and multinational enterprises.

ACS implements a status of the art softswitch for routing and managing ingress customers and egress suppliers. ACS is able to relay and control the STIR/SHAKEN signed calls. The development of the control and filtering features is constant and each new release a new more efficient and stringent procedure is released.

Robocall Mitigation Plan

This Robocall Mitigation Plan describes the specific measures that ACS has implemented to detect and prevent illegal robocalls on its network as of February 28, 2023. ACS is at risk of exchanging illegal robocalls principally if it is passed such traffic from its upstream carrier customers. The measures described below explain how ACS mitigates and addresses that risk, recognizing that it is impossible to prevent all illegal robocalls. ACS will periodically evaluate the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described. Should it determine that changes are appropriate, its practices may differ from those described below.

ACS, in accordance with the industry view (e.g., GSMA, I3Forum), does not view in general robocalls as a type of fraud and its approach to detection and mitigation of illegal robocalls, as potential driver of fraud attempts, relies in large part on ACS anti-fraud practices and protections. ACS vigorously monitors its traffic for signs of fraud. When potential fraud is

detected or when fraud is reported to ACS, ACS will investigate the source and circumstances of the traffic and will implement measures to block such traffic from recurring on the network. ACS works with a variety of industry stakeholders, including the ITG, the i3Forum, and CBAN to prevent fraud, including illegal robocalling.

Customer Due Diligence (KYC)

- ACS conducts a comprehensive due diligence and credit review before establishing a contractual relationship with carrier customers.
- ACS researches its carrier customers' reputation and assesses the accuracy of all reported information.
- ACS collects sufficient information to verify customer information is current when contracts are renewed or services are added.
- ACS will terminate or suspend service to customers with a history of non-compliance with its contractual obligations, including provisions relating to acceptable use of the service.

Measures to Prevent or Avoid Exchanging Illegal Robocalls

- **Contractual Provisions** – ACS contracts typically establish a reciprocal general obligation between ACS and its carrier customers to not use the services for any unlawful purpose, to prevent fraudulent uses, and to cooperate with each other to avoid these unlawful activities. ACS contracts also include a fraud clause, which follows the i3forum model and stipulates the legal actions ACS can take in case of receiving fraudulent traffic. The clause establishes: (a) the definition of what constitutes fraud; (2) liability and payment rules when fraud is found; (3) a right to suspend service; (4) the ability to initiate a dispute and dispute resolution procedures; and (5) credit note handling principles.
- **Fraud Detection** – ACS is fully engaged in the fight against illegal robocalling, CLI spoofing as a means to engage in fraud. ACS has created inter-working groups with the participation of stakeholders from several departments, including Security, Engineering, Product Management, Operations and Legal, in order to develop and support activities to mitigate illegal robocalling, spoofing and other fraud. ACS representatives participate in international anti-fraud forums to share information and employ best practices for countering robocalling and CLI spoofing. The ACS anti-fraud group functions 24 hours a day, 7 days a week and manages the search and detection of fraudulent traffic as well as escalation and notifications when such traffic is identified.
- **Blocking** – ACS blocks traffic from invalid numbers in case of any evidence or report by ITG. ACS also will block traffic that appears to be illegal or is flagged as suspicious under its fraud policy.

Responding to Traceback Requests

- ACS participates in the Industry Traceback Group (ITG).
- ACS follows the relevant ITG Best Practices to facilitate its response to traceback requests, including specifically:
 - **Dedicated Point of Contact** – ACS has designated an individual as a dedicated point of contact for addressing traceback requests, and a backup person to that individual, and has provided the ITG with the contact information and business hours for those individuals.
 - **Ongoing Coordination** – ACS will coordinate with the ITG and other voice service providers in relation to instances of suspicious traffic, including exchanging information related to such traffic and ad hoc follow-up as appropriate.
 - **Prompt Investigation and Response** – Upon receiving a traceback request from the ITG, ACS will endeavor to initiate investigation of the source of suspicious traffic within four (4) business hours after receiving a traceback request and strive to complete the investigation and response to the request through the traceback portal within 24 hours. In the event ACS is unable to respond to a traceback request, it will provide sufficient information in the traceback portal as to why it is unable to respond.
 - **Privacy of Traceback Investigations** – ACS will not share information about traceback investigations, except with the ITG, with other providers involved in the traceback investigation, or when pursuant to a valid legal process.
- ACS maintains current and correct information about its upstream carrier customers so that it can provide accurate responses to traceback requests.
- ACS performs preventive blocking of calls to U.S. destinations by providers listed as “non-responsive” by the ITG. ACS also performs blocking of calls to U.S. destinations by providers on the ITG “blacklist.”
- ACS will periodically review records of traceback requests to identify customers that are the subject of repeated traceback inquiries. ACS will determine an appropriate action to take on a case-specific basis, which may include working with the customer to mitigate illegal traffic, temporary suspension of the customer and/or termination of the customer’s service.
- ACS maintains records of any traceback request it receives and the carrier customer involved in the request.

Cooperation with State and Federal Regulators

ACS will cooperate with state and federal regulators to prevent any and all illegal robocalls. Specifically, ACS will:

- Respond to request for information about illegal robocalls;
- Provide relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities; and
- Implement mandated robocall mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls.