

Robocall Mitigation Program Description

AICEPTION LTD - FCC Robocall Mitigation Database Filing Attachment

Important filing note. This document is a draft program description prepared for AICEPTION LTD based on the operational information provided. It is intended to describe concrete robocall mitigation practices for inclusion as a PDF attachment in a Robocall Mitigation Database filing. Before submission, AICEPTION LTD should confirm the accuracy of all facts, complete any remaining placeholders, and obtain legal/regulatory review as appropriate. An authorized officer is responsible for the RMD certification submitted under penalty of perjury.

1. Provider Identification and Scope

Provider legal name	AICEPTION LTD
Business names / d/b/a names	AICEPTION LTD. No separate d/b/a name has been provided.
Responsible robocall mitigation contact	Richard Michael Gray. Title, business address, telephone number, and email address to be completed in the RMD filing.
Provider role(s)	AICEPTION LTD provides outbound VoIP voice services and originates outbound international traffic for customers using IP-based SIP interconnection. To the extent AICEPTION LTD acts in more than one call-path role, this program applies to each applicable role and to all traffic it originates, processes, or hands off to downstream carriers.

This program applies to all outbound voice traffic sent through AICEPTION LTD systems, including production CLI routes, customer accounts, IP-authenticated SIP trunks, FreePBX/Asterisk infrastructure, and any upstream or downstream provider relationships used for call completion.

Operational element	AICEPTION LTD profile
Approximate outbound volume	Around 100,000 outbound minutes per month
Outbound capacity	Minimum 50 concurrent outbound channels
Switching platform	FreePBX / Asterisk
SIP access control	SIP via IP authentication with static IP addresses
Codecs	G.711 and G.729
Traffic profile	International outbound traffic, mainly USA, UK, and Europe
Production caller ID policy	CLI routes only for production traffic

2. Certification Coverage

AICEPTION LTD confirms that all calls it originates or processes on its network are subject to this robocall mitigation program. The program is designed to prevent, detect, investigate, and stop illegal robocalls, unlawful spoofing, fraudulent traffic, and other abusive voice traffic.

STIR/SHAKEN status: To be completed in the RMD filing based on AICEPTION LTD's actual implementation status and eligibility. For any traffic or network segment for which AICEPTION LTD does not itself sign calls, AICEPTION LTD applies the mitigation practices described in this document and works with upstream/downstream providers to support caller ID authentication and traceability where technically feasible.

3. Customer Onboarding, KYC/KYB, and Account Approval

AICEPTION LTD does not activate production outbound CLI routes until the customer and use case have been reviewed and approved. The onboarding process includes the following controls:

- Verification of the customer legal name, registration details, business address, website/domain, and primary business contacts before enabling outbound service.
- Collection of intended traffic profile, calling use case, target countries, expected volume, concurrent channel requirements, and sample scripts or campaign descriptions when applicable.

- Assessment of whether the proposed use case is consistent with lawful calling requirements, including consent-based calling rules, do-not-call obligations, caller ID requirements, and destination-specific rules for the USA, UK, Europe, and other destinations served.
- Screening of customers and principals against internal risk indicators, complaint history, prior terminations, sanctions or enforcement concerns where available, and unusually high-risk business models.
- Requirement that each customer agree in writing that it will not originate illegal robocalls, unlawful spoofing, scam traffic, fraudulent calls, unsolicited high-risk campaigns, or traffic that violates destination-country rules.
- Activation of service only after AICEPTION LTD has documented the customer, approved the use case, and assigned appropriate route, channel, and caller ID controls.

4. Caller ID / CLI Management

AICEPTION LTD uses production routes that require CLI. AICEPTION LTD prohibits the use of false, misleading, invalid, or unauthorized caller ID information. CLI management controls include:

- Customers must provide evidence that they are authorized to use the telephone numbers presented as caller ID, such as ownership records, number assignment records, written authorization, or other reasonable proof.
- AICEPTION LTD may require test calls and sample traffic before enabling a new CLI, campaign, or destination profile.
- AICEPTION LTD blocks or rejects calls using malformed, invalid, anonymous, unallocated, premium-rate, emergency, or clearly spoofed caller ID values when detected.
- CLI changes for production traffic are reviewed and logged. Bulk CLI changes or unusual caller ID patterns trigger additional review.
- Customers may not rotate caller IDs to evade blocking, consumer complaints, analytics systems, or enforcement activity.
- Where technically feasible, AICEPTION LTD supports caller ID authentication requirements through provider coordination, customer documentation, traceability controls, and signing/attestation procedures appropriate to its network role.

5. Network Security and Access Controls

AICEPTION LTD operates FreePBX/Asterisk infrastructure with IP-authenticated SIP access using static IP addresses. The security objective is to ensure that only approved traffic from authorized sources can access outbound routes.

- Outbound SIP access is limited to known static customer IP addresses or authorized interconnection IPs.
- Unknown or unauthorized source IPs are not permitted to originate production outbound traffic.
- Administrative access to FreePBX/Asterisk systems is restricted to authorized personnel and protected using strong authentication practices and access controls.
- Route permissions, channel limits, trunk assignments, and destination access are configured according to the approved customer use case.
- Capacity controls are used to limit exposure, including concurrent channel limits and destination restrictions where appropriate.
- Logs and configuration records are maintained to support investigation and traceback of suspicious traffic.

6. Traffic Monitoring and Abuse Detection

AICEPTION LTD monitors outbound traffic patterns to identify suspicious or unlawful calling behavior. Monitoring is proportionate to its traffic volume and network role, including approximately 100,000 outbound minutes per month and at least 50 concurrent outbound channels.

- Unusual spikes in call volume, call attempts, short-duration calls, or answer-seizure ratio anomalies.
- High complaint levels, repeated call blocking, traceback notices, downstream carrier warnings, or regulator inquiries.
- Traffic to destinations inconsistent with the approved customer use case.
- Use of unauthorized, invalid, or rapidly changing caller IDs.
- Patterns associated with scam campaigns, spoofing, vishing, lead-generation abuse, or repeated failed calls.
- Outbound activity that materially exceeds approved channel, destination, or volume expectations.

7. Investigation, Blocking, Suspension, and Remediation

When AICEPTION LTD identifies suspected illegal robocalling, unlawful spoofing, fraud, or abusive traffic, it will take proportionate remedial action. Available actions include:

- Review call detail records, SIP logs, source IPs, caller IDs, destination patterns, customer account records, and route configuration.
- Request documentation from the customer, including consent evidence, CLI authorization, campaign description, call scripts, or customer remediation plan.
- Temporarily block specific caller IDs, destinations, routes, trunks, source IPs, or customer traffic while the issue is investigated.
- Reduce channel limits or restrict destinations for high-risk customers or campaigns.
- Suspend or terminate customers that originate illegal traffic, fail to cooperate, evade controls, or fail to cure violations.
- Notify relevant upstream or downstream providers where appropriate and cooperate with authorized tracebacks, regulator requests, and law-enforcement inquiries.

8. Traceback, Record Retention, and Cooperation

AICEPTION LTD maintains call and account records reasonably necessary to support traceback and mitigation. Records may include customer identity materials, service agreements, use-case approvals, CLI authorization records, static IP assignments, route configuration data, call detail records, SIP logs where available, complaint history, and investigation notes.

AICEPTION LTD will respond promptly and in good faith to traceback requests, Commission inquiries, law-enforcement requests, and notices from upstream/downstream carriers concerning suspected illegal robocalls. AICEPTION LTD will use available records to identify the customer, source IP, caller ID, route, destination, and relevant timestamps associated with the traffic at issue. The responsible contact for such matters is Richard Michael Gray, with additional RMD contact details to be completed in the filing.

9. Provider Vetting and Interconnection Controls

AICEPTION LTD reviews upstream and downstream voice providers used to complete traffic. The review is designed to ensure that interconnection partners support traceability and do not knowingly carry unlawful traffic. AICEPTION LTD may consider whether providers are listed in the FCC Robocall Mitigation Database where applicable, whether they respond to tracebacks, their reputation, routing quality, complaint history, and willingness to cooperate in mitigation.

AICEPTION LTD reserves the right to stop sending traffic to, or accepting traffic from, any provider or customer relationship that materially increases robocall risk, fails to cooperate with tracebacks, or threatens the integrity of the network.

10. Customer Contractual Requirements and Enforcement

AICEPTION LTD requires customers to comply with all applicable laws, regulations, and industry requirements governing outbound calling, consent, do-not-call lists, caller ID, privacy, telemarketing, emergency calling restrictions, and fraud prevention. Contractual and operational enforcement measures include:

- Acceptable use restrictions prohibiting illegal robocalls, scam calls, phishing/vishing, spoofing, harassment, fraudulent traffic, and attempts to evade analytics or blocking.
- Requirement to maintain evidence of consent and lawful basis for calls, particularly for marketing or lead-generation traffic.
- Requirement to use only authorized and accurate caller ID information.
- Right for AICEPTION LTD to audit, request documentation, suspend service, block traffic, reduce capacity, or terminate accounts based on risk or non-compliance.
- Requirement that customers cooperate with investigations, tracebacks, carrier notices, regulator inquiries, and remediation requests.

11. Ongoing Review and Program Updates

AICEPTION LTD reviews this robocall mitigation program periodically and when there are material changes to its network, traffic profile, customer base, routing partners, regulatory obligations, or observed abuse patterns. The company updates controls as needed based on complaint trends, traceback experience, carrier feedback, changes in FCC or destination-country requirements, and operational lessons learned.

AICEPTION LTD will update its Robocall Mitigation Database submission within the required timeframe if any required information materially changes, including responsible contact information, provider role, business names, STIR/SHAKEN status, affiliations, enforcement history, or this mitigation program description.

12. Attestation

AICEPTION LTD attests that the practices described above are intended to reasonably mitigate the origination, processing, and transmission of illegal robocalls and unlawful spoofing on its network. AICEPTION LTD will apply these controls to all covered outbound traffic and will take corrective action when illegal or suspicious traffic is detected.

Authorized officer/contact name:	Richard Michael Gray
Title:	To be completed
Date:	To be completed
Signature:	Handwritten or authorized electronic signature to be added by Richard Michael Gray.

13. Public Filing Reference Basis

This program description is prepared to align with FCC Robocall Mitigation Database filing requirements requiring PDF upload of the mitigation program description and requiring providers to describe specific reasonable practices to mitigate illegal robocalls. This document avoids relying on generalized statements alone and instead identifies specific onboarding, caller ID, monitoring, traceback, suspension, and enforcement practices.