

Robocall Mitigation Program Description

AZRAK / Azrak International

Document Date:	February 14, 2026
Purpose:	Program description to support Robocall Mitigation Database (RMD) filing under 47 CFR § 64.6305(a) and related provisions.
STIR/SHAKEN Status:	No STIR/SHAKEN implementation by filer (Option 3) – lack of control over network infrastructure
Upstream Platform:	SkySwitch (upstream VoIP platform/provider)

Company Contact

Company:	Azrak International
Address:	100-1075 North Service Road West, Oakville, ON L6M 2G2, Canada
Phone:	1-866-300-5151
Email:	wecare@azrak.ca

Regulatory Reference

This program is maintained to support compliance with FCC robocall mitigation requirements applicable to voice service providers and to meet the obligations described in 47 CFR § 64.6305(a) and related provisions.

1. Scope and Applicability

AZRAK provides VoIP services to end users as a reseller using an upstream platform/provider. This Robocall Mitigation Program applies to all voice services provisioned by AZRAK and covers the operational controls used to prevent the origination of illegal robocall traffic, to investigate suspected abuse, and to cooperate with traceback requests.

2. STIR/SHAKEN Status and Basis for Option 3

Rule basis: Under 47 CFR § 64.6305(d)(2)(i), a filer that has not implemented STIR/SHAKEN may provide an explanation that it is unable to implement STIR/SHAKEN due to a lack of control over the network infrastructure necessary to implement STIR/SHAKEN.

AZRAK is a non-facilities-based reseller and does not own or operate the network elements required to deploy STIR/SHAKEN (including call authentication/signing infrastructure, interconnects, and core switching/SBC functions). Those elements are controlled by the upstream platform/provider. As a result, AZRAK cannot independently implement STIR/SHAKEN on any portion of the underlying network used to originate calls. Where caller ID authentication is available, it is implemented by the upstream provider as part of the platform/network.

3. Robocall Mitigation Controls

Customer Verification (KYC)

- Validate customer identity and contact information prior to activation (business name, address, authorized user, and reachable phone/email).
- Perform reasonable risk screening for high-risk use cases (high-volume outbound calling, lead generation, offshore dialing operations, etc.).
- Require accurate Caller ID information and prohibit caller ID spoofing or misrepresentation.

Acceptable Use and Contractual Enforcement

- Terms of service explicitly prohibit illegal robocalls, spoofing, and abusive calling patterns.
- AZRAK reserves the right to suspend or terminate service, and to block numbers/routes associated with suspected illegal robocalling.
- Customers must cooperate with investigations and provide requested information related to calling campaigns.

Traffic Monitoring and Abuse Detection

- Monitor usage and alerts for anomalies such as sudden volume spikes, repeated short-duration calls, high answer/seizure anomalies where available, and complaint-driven investigations.
- Apply controls appropriate to the platform capabilities (rate limits, outbound restrictions, and campaign review for high-risk accounts).
- Escalate suspected illegal traffic for immediate containment actions.

Complaint Handling and Investigation

- Maintain an abuse reporting channel and track complaints with timestamps, calling numbers, and customer identifiers.
- Investigate within business hours (and as quickly as feasible) and take immediate interim steps when strong indicators of illegal robocalling exist.
- Preserve logs and evidence relevant to the investigation.

Blocking, Suspension, and Remediation

- Promptly suspend impacted customer accounts/trunks/DIDs when illegal robocall activity is suspected or confirmed.
- Coordinate with the upstream provider to apply network-level blocks, disable routes, and stop traffic at the platform level.
- Require corrective actions (e.g., campaign documentation, opt-in proof) prior to reinstatement.

Upstream Coordination

- Maintain escalation contacts with the upstream provider for rapid containment and technical actions.
- Request upstream implementation of additional controls when patterns indicate emerging threats or new abuse vectors.

Traceback Cooperation

- Commit to respond fully and within 24 hours to traceback requests from the FCC, law enforcement, and the industry traceback consortium.
- Provide relevant account identifiers and call detail records available to AZRAK, and coordinate with the upstream provider for additional network records when needed.

Recordkeeping

- Retain customer onboarding records (KYC), service activation details, and abuse/complaint case notes for a reasonable period consistent with business and legal requirements.
- Retain relevant calling logs and suspension/remediation actions to support traceback and enforcement.

Training and Governance

- Train staff responsible for onboarding, support, and operations on identifying illegal robocall indicators and handling escalation workflows.
- Review this program periodically and update controls as platform capabilities or regulatory expectations evolve.

4. Traceback and Enforcement Workflow

Upon receipt of a traceback request, complaint, or credible notification of illegal robocalling, AZRAK follows the workflow below:

- 1 Log the request/complaint and acknowledge receipt.
- 2 Identify the customer/account and impacted numbers/routes using available records.
- 3 Apply immediate containment (suspend account/DIDs, restrict outbound calling, and/or request upstream blocking) when warranted.
- 4 Collect and preserve relevant call records and onboarding details.
- 5 Respond to the requesting entity with available details, and coordinate with the upstream provider for additional network records if required.
- 6 Maintain the case record and document final remediation and disposition.

5. Points of Contact

AZRAK designates the following organizational contacts for robocall mitigation, abuse handling, and traceback coordination (specific named individuals may be provided to counterparties upon request):

Role	Contact Method	Availability
Robocall Mitigation / Abuse Desk	wecare@azrak.ca	Mon-Fri business hours; urgent escalation support
Traceback Response	wecare@azrak.ca	Respond within 24 hours per 47 CFR § 64.630
Telephone	1-866-300-5151	Business hours

6. Certification Statement (Program Maintenance)

AZRAK maintains this Robocall Mitigation Program as a living document. Controls are reviewed periodically, and AZRAK will cooperate with the FCC, law enforcement, and the industry traceback consortium to investigate and stop illegal robocallers that use AZRAK's service to originate calls.

This document is intended to describe AZRAK's operational robocall mitigation practices and is provided for compliance purposes in connection with the Robocall Mitigation Database filing.