

IDRAK AI LLC

ROBOCALL MITIGATION PLAN

I. Background

The Federal Communications Commission ("FCC" or "Commission") has adopted rules requiring voice service providers, like IDRAK AI LLC ("IDRAK AI"), to, among other things, file certifications and robocall mitigation plans in the FCC's Robocall Mitigation Database ("RMD").

The FCC requires that all voice service providers certify in the Commission's RMD whether they have implemented the STIR/SHAKEN authentication framework, and that all of the calls that they originate, carry, or process are subject to a robocall mitigation program consistent with the Commission's rules.

The provider's mitigation plan shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

The Commission's rules and the TRACED Act address illegal robocalling, including violations of Sections 227(b) and 227(e) of the Communications Act. IDRAK AI's robocall mitigation efforts focus on preventing calls that violate the Telephone Consumer Protection Act (TCPA) and the Truth in Caller ID Act, including calls made using an automatic telephone dialing system or artificial or prerecorded voice in violation of applicable law, and calls that transmit misleading or inaccurate caller identification information with intent to defraud, cause harm, or wrongfully obtain anything of value.

The Commission has stated that a robocall mitigation program should include detailed practices that can reasonably be expected to significantly reduce the origination or carriage of illegal robocalls and that the provider should comply with the practices described in its plan.

IDRAK AI is committed to implementing commercially reasonable measures to prevent illegal robocall traffic and to comply fully with applicable FCC rules.

II. IDRAK AI's Know Your Customer (KYC) Standards

IDRAK AI is a voice service provider and wholesale intermediate provider, including both gateway and non-gateway services, focused on business and wholesale communications customers.

As part of its customer onboarding process, IDRAK AI undertakes commercially reasonable measures to verify customer identity, including completion of a KYC questionnaire, execution of a written service agreement, and collection of regulatory documentation where applicable.

IDRAK AI collects and verifies, as appropriate, the following customer information:

- Legal business name and entity type
- State or country of incorporation
- Physical business address
- Primary, technical, and compliance contacts with phone numbers and email addresses
- Trade and/or bank references
- Federal Tax ID number

- FCC Form 499 Filer ID and FRN
- Robocall Mitigation Database filing status
- Company website or other customer-facing presence

IDRAK AI verifies carrier customers through applicable FCC databases and the FCC Robocall Mitigation Database, conducts publicly available research regarding customer history, and reviews traceback history where applicable. New customer traffic is monitored for call patterns, ASR, ACD, caller ID usage, and other indicators of traffic hygiene concerns.

III. IDRAK AI's Acceptable Use Policy

All IDRAK AI customers are contractually bound by IDRAK AI's Acceptable Use Policy (AUP), which prohibits:

- Illegal, abusive, fraudulent, deceptive, or misleading activities
- Unsolicited or unlawful telemarketing and advertising
- Violations of the TCPA, FTC Telemarketing Sales Rule, FCC regulations, and state and federal Do-Not-Call laws
- Spoofing or misrepresentation of caller identity, including violations of the Truth in Caller ID Act

IDRAK AI reserves the right to suspend or terminate services for violations of its AUP.

IV. Telephone Number Authorization, STIR/SHAKEN & Attestation Logic

IDRAK AI maintains procedures intended to ensure that caller identification information and STIR/SHAKEN attestations are handled in accordance with applicable requirements and the information available regarding its customers and their authorization to use telephone numbers.

IDRAK AI expects customers to use telephone numbers they are authorized to use and may request supporting documentation where appropriate.

V. Proactive Network Monitoring

IDRAK AI employs internal and third-party analytics to monitor traffic for potential illegal robocall activity. Monitoring includes:

- Abnormal call volumes, pacing, ASR, and ACD
- NPA-NXX matching between calling and called numbers
- Calls from numbers on the Somos Do-Not-Originate list
- Media IP addresses linked to known illegal robocalling entities
- Wireless and high-risk destination analysis

IDRAK AI utilizes third-party tools including Somos DNO services, Fraud Central RoboGuard, and ZipDX RRAPTOR.

VI. Enforcement Workflow

1. Alert

Triggered by analytics, complaints, or traceback notifications. Customer is notified and traffic reviewed.

2. Suspend

Temporary suspension of traffic, caller IDs, or service. Customer is required to take corrective action.

3. Terminate

Permanent termination for confirmed or repeat violations. Notification to relevant partners when appropriate.

Enforcement actions may be accelerated based on severity or regulatory risk.

VII. Escalation & Repeat Offender Procedures

For repeat or serious violations, IDRAK AI may:

- Immediately block offending ANIs or traffic
- Terminate customer services
- Revoke or downgrade attestation privileges
- Increase monitoring of associated accounts
- Cooperate fully with regulatory and industry investigations

VIII. Commitment to Traceback Cooperation

IDRAK AI commits to responding within 24 hours to all traceback requests from the FCC, law enforcement, and the industry traceback consortium.

IDRAK AI will cooperate fully in investigations and take prompt corrective action when illegal robocall activity is identified.