

Dialect, LLC - ROBOCALL MITIGATION PLAN

UPDATED - FEBRUARY 2026

PURPOSE AND SCOPE

Dialect, LLC (the "Provider") is a voice service provider that originates voice traffic to the public switched telephone network (PSTN) and maintains a robocall mitigation program consistent with 47 CFR § 64.6305, including STIR/SHAKEN caller ID authentication implemented pursuant to 47 CFR § 64.6301(a).

PROVIDER ROLE / CALL FLOW

The Provider offers hosted voice services to business end-user customers. Outbound calls originate from end-user endpoints on the Provider's platform using telephone numbers assigned/provisioned by the Provider and are routed to the PSTN via upstream carrier partners. The Provider does not provide service to downstream voice service providers; its customer base is comprised of end-user businesses.

STIR/SHAKEN STATUS

The Provider certifies that it has implemented STIR/SHAKEN caller ID authentication across its network consistent with 47 CFR § 64.6301(a). The Provider's voice network is IP-based, and the Provider signs outbound calls it originates using its own STI certificate issued by an approved STI Certificate Authority (STI-CA), with call signing performed by the Provider's in-house developed signing software. For inbound SIP calls received for termination/delivery to end users where the caller identification information has been authenticated, the Provider verifies caller identification information where technically feasible.

The Provider assigns attestation levels based on its verification of the calling party and confirmation of the calling party's authority to originate calls using the associated telephone number(s), consistent with applicable FCC rules, orders, and guidance.

KNOW YOUR CUSTOMER PROCEDURES

The Provider takes affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence to ensure its services are not used to originate illegal traffic.

At onboarding, we collect and verify business identity and authority information, e.g., legal name or DBA, service address, authorized representative, contact details and perform a risk-based review as appropriate, which may include checking public business records where available, validating consistency of contact information, and confirming the reasonableness of the requested services and stated use case, including expected calling purpose, target geography, anticipated volumes, and general calling patterns.

Enhanced review is triggered by high-risk verticals, unusually high projected volume, discrepancies in identity, repeated changes to caller ID, short-lived accounts, or any indicators

inconsistent with the stated use case.

Additionally, customer agreements prohibit illegal robocalls, unauthorized caller ID/spoofing, misuse of numbering resources, and other unlawful or abusive calling activity, and reserve our right to investigate and take corrective action when suspicious or unlawful activity is identified.

TRAFFIC MONITORING, ANALYTICS, AND ENFORCEMENT

We monitor traffic patterns and call performance metrics with our internal systems to detect suspicious behavior, including burst calling, short-duration spikes, high invalid destinations, or irregular caller ID patterns. We also rely on upstream carrier analytics and enforcement signals, including robocall/spam indicators and blocking feedback, to identify potentially illegal or unwanted traffic. When suspicious or illegal traffic is detected, our escalation typically follows:

1. investigate and contact customer
2. warn and request remediation/supporting documentation
3. rate-limit or temporarily block affected traffic/caller IDs
4. suspend service if unresolved
5. terminate service for repeat or confirmed abuse, and we cooperate with upstream carriers and applicable traceback requests when required.

KNOW YOUR UPSTREAM PROVIDERS

The Provider does not accept third-party traffic for transit. Outbound calls originate only from the Provider's end users; inbound calls are received from carrier partner(s) only for delivery to those end users. The Provider coordinates with its upstream carrier partner(s) on suspected illegal traffic and traceback requests.

TRACEBACK COOPERATION AND PLAN GOVERNANCE

The Provider remains committed to responding fully and within 24 hours to call traceback requests from the Commission, law enforcement, and the traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers initiating calls.

The Provider has not been prohibited from filing a certification in the Robocall Mitigation Database.

The Provider reviews and maintains its robocall mitigation program and updates it within 10 business days when filing information, services, traffic patterns, or risk controls change.