

Adnet Media Group Inc - Robocall Mitigation Plan

Updated February 20, 2026

Robocall Mitigation Plan Summary:

Adnet Media Group Inc (the “Provider”) is a voice service provider that originates 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).

STIR/SHAKEN Implementation Details:

The Provider certifies that it has implemented STIR/SHAKEN caller ID authentication across the IP portions of its network for the SIP calls it originates, consistent with 47 CFR § 64.6301(a). The Provider’s STIR/SHAKEN deployment includes a valid Service Provider Code (SPC) token, an STI certificate issued by an approved Certificate Authority (Telonium), and an operational authentication infrastructure.

All IP-based calls originated by the Provider that ultimately terminate on the PSTN are signed using the Provider’s STIR/SHAKEN certificate. The Provider uses Prescott-Martini Group solely to perform the technical act of signing; however, the Provider retains sole responsibility for attestation selection and compliance with the Commission’s STIR/SHAKEN rules and applicable technical standards. The Provider determines the attestation level based on its verification of the calling party and the calling party’s authority to use the associated telephone number(s), and maintains controls designed to help prevent caller ID spoofing and illegal robocall traffic.

Robocall Mitigation Measures:

a. Know Your Customer Procedures

The Provider’s end-user customers consist of small businesses, including lawyers, hotels, doctors, and professional services. The Provider maintains a Know Your Customer (KYC) program to help prevent new and renewing customers from using its network to originate illegal calls. At onboarding, the Provider collects and verifies business identity information, as applicable, including legal business name/DBA, EIN and/or formation documents, service address, authorized representative, primary contact details, and payment credentials.

Customer approval includes a risk review, which may include checks of publicly available business records, consistency of submitted information, and the stated use case, expected volumes, and calling patterns prior to enabling outbound calling. Enhanced review is triggered by higher-risk verticals, unusually high projected volume, discrepancies in identity or authority, frequent caller ID changes, short-lived accounts, or other indicators of lead-generation/robocall behavior inconsistent with the stated use case.

The Provider’s Terms of Service and Acceptable Use Policy prohibit illegal robocalls, spoofing/unauthorized caller ID, and other unlawful or abusive activity, and reserve the Provider’s right

to investigate, require documentation, and rate-limit, block, suspend, or terminate service for suspected or confirmed violations.

b. Traffic Monitoring and Enforcement

The Provider monitors outbound calling activity using in-house tools and operational reviews to identify anomalous or suspicious behavior. Monitoring focuses on indicators such as sudden traffic spikes or bursts, abnormal ASR/ACD, short-duration call surges, elevated invalid/unallocated destination attempts, and inconsistent or invalid caller ID patterns. Customer access is restricted to authenticated IP addresses, and geoIP controls are used to block international calling, which reduces exposure to common fraud vectors. The Provider relies on internal monitoring only and does not use third-party analytics vendors for traffic scoring or blocking decisions.

When potentially illegal or abusive activity is identified, the Provider follows a defined escalation process: (i) investigate and contact the customer; (ii) warn and request remediation and/or supporting documentation; (iii) rate-limit or temporarily block impacted traffic streams and/or caller IDs; (iv) suspend service if unresolved; and (v) terminate service for repeat or confirmed abuse. The Provider cooperates with applicable traceback requests and works with its carrier partner(s) as needed to support investigation and remediation.

c. Know Your Upstream Providers

For purposes of this plan, this section describes the Provider's due diligence for the carrier partner(s) to which it hands off originating traffic for PSTN termination. The Provider does not accept or transit third-party provider traffic; all traffic handled is generated by the Provider's own end-user customers on its hosted PBX platform. For outbound calls, the Provider delivers originating traffic to one or more carrier partners for PSTN interconnection/termination (i.e., the next provider(s) in the outbound call path). The Provider maintains current escalation and traceback points of contact with those carrier partners, confirms the availability of call detail records needed to support investigations and traceback, and periodically reviews partner performance and fraud/robocall indicators, including in response to suspected illegal traffic events.

Traceback Commitment and Plan Maintenance:

The Provider has identified a single point of contact for traceback cooperation and 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, including providing relevant call records and supporting information as requested. In addition, 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 to ensure the filing remains accurate, complete, and current.