



A1ROUTES LLC

Robocall Mitigation Plan

Updated – February 27, 2026



The following is A1ROUTES LLC submission to the Robocall Mitigation Database, pursuant to the FCC's directive.

A1ROUTES LLC is a USA IPES operator registered in Texas, USA

Indicated below are the robocall mitigation measures employed by A1ROUTES switching platform.

24 Hour Response

A1ROUTES certifies that it will respond to all traceback requests from the industry traceback group (ITG) within 24 hours and civil and criminal law enforcement agencies, cooperating fully in efforts to investigate and eliminate robocalls, while following CPNI requirements.

STIR/SHAKEN Implementation

A1ROUTES has fully implemented STIR/SHAKEN attestation. All compliance or questions with the RMD or STIR/SHAKEN should be reported to regulatory@a1routes.com

A1ROUTES RMD Verification

A1ROUTES policies require refusing traffic from any other provider not registered in Robocall Mitigation Database

A1ROUTES KYC Verification

A1ROUTES performs customer due diligence and KYC, mandating that all potential customers complete a KYC form and undergo a due diligence process. That include online verification of their ID proof and Address proof on file.

A1ROUTES Mitigation certification

A1ROUTES certifies that all calls originating on our network are subjected to a robocall mitigation program that meets specified requirements. We affirm that our prior certifications remain



unrevoked by Commission action and that we are not barred from participation in the Robocall Mitigation database.

Telephone Number Authorization

A1ROUTES Telephone Number (TN) authorization is based on our direct assignment of TN to our customer purchase through us. When originating a call, A1ROUTES checks the calling party number against A1ROUTES' inventory and will provide appropriate attestation to the call based on industry standards.

If a A1ROUTES customer wishes to use a TN as caller identity and that A1ROUTES does not directly manage TN, then attestation adjustments can be made if A1ROUTES customer meets the following conditions:

They are an existing A1ROUTES customer with KYC verified. And can provide proof of ownership of number, and they have not received industry complaints (tracebacks, vendors) in their tenure with A1ROUTES.

A1ROUTES blocks all traffic with invalid and 3rd party ANIs

DNO Compliance

A1ROUTES has protocols in place to detect DNO calls and block those calls.

Regulatory Compliance

A1ROUTES is not currently, nor has it ever been subject to any commission law enforcement or regulatory agency action or investigation related to suspected unlawful robocalling or spoofing activities.

Traffic Monitoring

A1ROUTES monitors traffic on the Web and utilizes various control processes to identify Robocall call groups. We consistently analyze the CDRs (Call Detail Record) and live calls to detect patterns associated with this practice, such as numbers of similar series, trunks attempting to exceed typical conversational CPS, a high number of short duration calls or calls to invalid numbers. Daily CDR review and automated internal reports allow us to detect and investigate suspicious traffic.

Action:

If these calls are identified, we implement the following procedures:

1. Immediately notify customer of the offending traffic and open a ticket to track the issue.



2. Block the offending traffic by number, IP address or trunk group until we receive confirmation from our customer that traffic has been permanently removed from their network.
3. Implement close monitoring of the trunk for the next (72) hours to confirm that the traffic has indeed been successfully removed.
4. Respond to any traceback requests from the Commission, the police and the registered traceback consortium and collaborate with these entities in the investigation and detection of any illegal robocalls transmitted using our network.