

EXORDIUM NETWORKS INC - ROBOCALL MITIGATION PLAN

UPDATED FEBRUARY 2026

This Robocall Mitigation Plan describes the policies and procedures Exordium Networks Inc (the “Provider”) uses to prevent, detect, and mitigate illegal robocall traffic consistent with 47 C.F.R. § 64.6305 and related FCC guidance.

This plan applies to all calls originated by the Provider’s customers using the Provider’s hosted PBX and SIP trunking services, including enterprise customers such as senior living operators. This plan also applies to the limited reseller traffic that originates from PBX services hosted and controlled by the Provider.

The Provider reviews and maintains this Robocall Mitigation Plan and will update its Robocall Mitigation Database filing within 10 business days of any changes to its filing information, services, traffic patterns, or mitigation controls.

Provider Role

The Provider offers hosted PBX and SIP trunking services and assigns/maintains customer DIDs through upstream carrier partners.

Customers are primarily small and mid-sized businesses and senior living operators (the operator is the Provider’s direct customer and may extend calling capability to residents). The Provider also supports one reseller using a PBX hosted on the Provider’s platform.

Outbound calls are placed by customer endpoints and/or PBX systems, hosted by the Provider or located on customer premises, routed through the Provider’s platform, signed by the Provider, and then delivered to upstream carrier partners for termination to the PSTN. Inbound calls to Provider-assigned DIDs are received from upstream carriers and delivered to the appropriate customer endpoints.

STIR/SHAKEN Implementation

The Provider certifies that it has implemented Complete STIR/SHAKEN caller ID authentication consistent with 47 C.F.R. § 64.6301(a). The Provider’s voice network is entirely IP-based, and the Provider authenticates and signs 100% of outbound calls it originates using its own STI certificate issued by an approved STI Certificate Authority (STI-CA) with an in-house signing solution (i.e., the signing function is performed on Provider-controlled servers and is not provided by a third-party hosted signing vendor).

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

The Provider uses a risk-based onboarding process for new customers. At onboarding, the Provider collects billing information and the end-user service address. Customers are onboarded under contract terms that include acceptable use restrictions and provide the Provider the right to suspend or terminate service for suspected illegal or abusive calling activity.

The Provider confirms the customer's intended use case during onboarding. Service is primarily used for business calling and limited personal use.

Enhanced review is required when a customer indicates, or the Provider otherwise identifies, a higher-risk calling profile, including planned high-volume or large-scale marketing/dialing activity.

Traffic Monitoring and Analytics

The Provider monitors outbound calling activity and relies on alerts and notifications from its upstream carrier partners when suspicious calling patterns are identified. When an alert is received, the Provider reviews available call records and customer activity to validate the issue and identify the responsible customer.

If suspicious or illegal traffic is detected, the Provider takes prompt mitigation action. Typical escalation includes:

- (1) block the affected traffic and/or calling number(s),
- (2) notify and escalate to the customer's designated point of contact,
- (3) require immediate remediation and, where appropriate, supporting explanation/documentation, and
- (4) maintain the block, suspend service, or terminate service for repeated or unresolved violations.

Additionally, the Provider maintains Terms of Service and an Acceptable Use Policy that prohibit illegal robocalls, spoofing or unauthorized caller ID, misuse of numbering resources, and other unlawful or abusive calling activity. Customer agreements reserve our right to investigate and to block, suspend, or terminate service for suspected or confirmed violations.

Know Your Upstream Provider

The Provider generally does not accept traffic from upstream providers or third-party partners. The Provider supports one limited reseller relationship that uses a Hosted PBX instance on the Provider's platform. The Provider retains administrative control over the hosted PBX environment and call routing, and the reseller's traffic is subject to the Provider's Terms of Service/Acceptable Use restrictions and the same monitoring and mitigation procedures applied to customer-originated traffic.

Traceback Commitment

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.

