



**CONNEXPLUS CORP.
ROBOCALL MITIGATION PLAN
UPDATED - FEBRUARY 2026**

PURPOSE AND SCOPE

This Robocall Mitigation Plan (the “Plan”) describes the policies, procedures, and controls used by CONNEXTPLUS CORP. (the “Provider”) to prevent, detect, investigate, and mitigate illegal robocall activity associated with calls originated using the Provider’s services, pursuant to 47 CFR § 64.6305.

This Plan applies to all outbound voice traffic originated by the Provider’s business end-user customers through the Provider’s SkySwitch-hosted environment, including calls placed from provisioned extensions/devices and using numbering resources assigned to customers. It also covers customer onboarding controls, monitoring and escalation procedures, and traceback cooperation.

PROVIDER ROLE AND STIR/SHAKEN STATUS

The Provider serves only business enterprise end users and does not provide service to other voice service providers, resellers or wholesale customers.

The Provider’s voice operations are hosted on the SkySwitch platform. The Provider does not operate its own STIR/SHAKEN signing function, does not maintain its own STI certificate, and does not independently authenticate calls outside of the SkySwitch-hosted environment. STIR/SHAKEN authentication for calls originating on the SkySwitch platform is performed within SkySwitch-controlled infrastructure as part of their implementation. The Provider relies on this hosted implementation and maintains a robocall mitigation program consistent with 47 CFR § 64.6305.

KNOW YOUR CUSTOMER PROCEDURES

The Provider uses risk-based customer onboarding and account oversight designed to reduce the likelihood that customers use the services to originate illegal calls.

At onboarding, and as needed thereafter, the Provider collects and verifies business identity and authority information as appropriate, which may include legal name/DBA, EIN and/or formation documentation, service address, authorized representative, contact information, and payment method. Prior to enabling outbound calling, or enabling increases in calling capability, the Provider collects the stated use case and expected calling profile and reviews the request for consistency and reasonableness.

Enhanced review may be triggered by high-risk verticals, unusually high-volume requests, identity discrepancies, frequent caller ID changes, short-lived accounts, or other indicators inconsistent with the stated use case.

The Provider’s Terms of Service and Acceptable Use Policy prohibit illegal robocalls and spoofing and reserve the right to request supporting documentation and to block, suspend, or terminate service where warranted.



TRAFFIC MONITORING, ANALYTICS, AND ENFORCEMENT

The Provider uses SkySwitch reporting tools, including access to call detail records and platform diagnostics, to review outbound calling activity for indicators of misuse. The Provider investigates issues identified through platform reporting, customer complaints, upstream notifications, or traceback requests.

If suspicious or illegal traffic is detected, mitigation actions may include customer outreach, warnings and remediation requests, requests for supporting documentation, temporary rate limits or blocks, including by caller ID, suspension of service, and termination for repeated or confirmed abuse.

KNOW YOUR UPSTREAM PROVIDER

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 RESPONSE

The Provider maintains a point of contact for traceback cooperation and commits to responding fully and within 24 hours to traceback requests from the FCC, law enforcement, and the industry traceback consortium, including providing relevant call records and supporting information as requested.

PLAN MAINTENANCE AND GOVERNANCE

The Provider reviews this Plan periodically and updates its RMD filing and associated plan information within 10 business days of material changes to filing information, services, traffic patterns, or relevant controls.