

ROBOCALL OVERSIGHT AND CALL AUTHENTICATION POLICY

STIR/SHAKEN Compliance

Ringlytics delivers voice communication services and manages approximately 100,000 subscriber voice lines. On this basis, Ringlytics qualifies for and operates under a STIR/SHAKEN implementation extension as allowed by 47 CFR § 64.6304.

Most outbound traffic transmitted across Ringlytics' network is authenticated through STIR/SHAKEN protocols. Any calls that are not verified are handled under the robocall mitigation measures described below.

Robocall Monitoring and Action

Ringlytics utilizes network monitoring and fraud detection controls to identify suspicious or unlawful robocall behavior. These controls detect calls originating from invalid, unassigned, or non-operational caller ID numbers.

When such activity is observed, Ringlytics immediately restricts or blocks the affected traffic and performs an internal review. If a customer is found to be attempting unlawful robocalls, Ringlytics issues a notice directing the customer to cease such activity. Continued violations may result in suspension or termination of service.

Traceback Cooperation

Ringlytics responds to traceback requests from the FCC, law enforcement agencies, and the registered traceback consortium within 24 hours. Ringlytics works cooperatively with these entities to trace the source of illegal robocalls and prevent further misuse.

Customer Review and Vetting

Ringlytics follows customer vetting practices aligned with the NANC Call Authentication Trust Anchor Working Group. During onboarding, Ringlytics evaluates each customer's intended service use and expected calling volume. At present, Ringlytics does not onboard customers whose primary purpose involves high-volume outbound calling.