

Robocall Mitigation Program Description

Company Overview

Replify provides an application-layer communications platform that enables businesses to interact with customers via voice and messaging. Replify does not operate its own telecommunications network and relies on upstream providers such as Twilio for call origination and termination.

STIR/SHAKEN Status

Replify does not implement STIR/SHAKEN directly. All STIR/SHAKEN authentication is handled by upstream providers, including Twilio. As such, Replify is not subject to a direct STIR/SHAKEN implementation obligation under 47 CFR § 64.6301.

Robocall Mitigation Practices

Replify maintains a robocall mitigation program designed to prevent illegal robocalls, including: - Requiring express consent and opt-in for outbound communications - Monitoring call and messaging traffic for suspicious patterns - Enforcing customer compliance with applicable laws (TCPA, FCC rules) - Suspending or terminating accounts that violate policies - Maintaining audit logs and call records for investigation

Traceback Cooperation

Replify commits to responding fully and within 24 hours to traceback requests from the FCC, law enforcement, and the Industry Traceback Group. Replify will cooperate in investigating and mitigating any illegal robocall activity.

Upstream Provider Reliance

Replify relies on upstream providers, including Twilio, for network-level protections, including STIR/SHAKEN and traffic validation.

Ongoing Compliance

Replify continuously evaluates and improves its mitigation practices and ensures alignment with FCC requirements and evolving industry standards.