
Short-Form Robocall Mitigation Program Description (Option 1)

r2d10 has fully implemented the STIR/SHAKEN authentication framework across its entire IP-based network. All calls originated on our network are authenticated and signed in compliance with 47 CFR § 64.6301. No unsigned outbound traffic is permitted.

In addition to full STIR/SHAKEN implementation, r2d10 maintains a robocall mitigation program consistent with 47 CFR § 64.6305(a). Our mitigation measures include:

- Know-Your-Customer (KYC) procedures to verify the identity and legitimacy of customers prior to service activation
- Enhanced due diligence for high-volume or higher-risk customers
- Real-time and post-origination traffic monitoring to detect anomalous calling patterns, high-volume short-duration calls, invalid or unallocated number usage, and potential spoofing
- Blocking of invalid, unallocated, or unauthorized numbers
- Immediate investigation and mitigation of suspicious traffic

We retain call detail records sufficient to support traceback investigations and commit to respond fully and within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement, and the Industry Traceback Consortium. Confirmed illegal robocall activity results in immediate remediation, including suspension or termination of service when appropriate.

This mitigation program is reviewed periodically and updated as necessary to ensure continued compliance with applicable FCC rules and evolving industry best practices.