



Robocall Mitigation Plan (RMP)

Quantum Com LLC

August 2025

1. Executive Summary

Quantum Com LLC (“Quantum”) is a United States-based telecommunications service provider, duly registered with the Federal Communications Commission (FCC), and committed to delivering lawful, secure, and trusted voice communications. This Robocall Mitigation Plan (“RMP”) is submitted to the FCC’s Robocall Mitigation Database in accordance with 47 CFR § 64.6305 and outlines the comprehensive controls Quantum employs to detect, prevent, and mitigate illegal robocalls on its network.

Illegal robocalls are one of the most significant threats to consumer trust in the U.S. voice ecosystem. Fraudulent robocalls erode public confidence, harm vulnerable consumers, and impose significant costs on carriers and enterprises alike. Recognizing this, Congress enacted the TRACED Act (Telephone Robocall Abuse Criminal Enforcement and Deterrence Act) and the FCC has since mandated provider-level mitigation measures, including STIR/SHAKEN call authentication and formalized robocall mitigation programs. Quantum has developed a robust, multi-layered strategy that exceeds minimum regulatory requirements.

This plan is based on three guiding principles:

- A) Prevention through Customer Vetting and Onboarding Controls:** Every prospective customer is subjected to stringent Know Your Customer (KYC) and Know Your

Business (KYB) verification. No customer is activated without proof of lawful identity, corporate existence, and verified authority over calling numbers.

B) Continuous Monitoring and Automated Analytics

Quantum employs advanced real-time traffic monitoring, behavioral analytics, and anomaly detection to identify suspicious patterns. Short-duration bursts, high calls-per-second (CPS), sequential dialing, or sudden traffic spikes trigger automated alerts and may result in blocking.

C) Swift Enforcement and Cooperative Response

Quantum acts decisively when illegal traffic is suspected, suspending or terminating offending accounts, fully cooperating with the Industry Traceback Group (ITG), and notifying regulators when necessary.

This document provides a detailed explanation of our mitigation practices across the lifecycle of call traffic — from onboarding and attestation, to monitoring and enforcement, to traceback cooperation and ongoing compliance governance.

Quantum certifies under penalty of perjury that the following mitigation practices are fully implemented and operational, and that we will maintain and adapt this plan as industry standards and FCC rules evolve.



Robocall Mitigation Plan (RMP)

Quantum Com LLC

August 2025

2. Company Overview:

- **Legal Name:** Quantum Communications LLC
- **Jurisdiction of Incorporation:** Florida, United States
- **FCC Registration Number (FRN):** 39-3520854
- **499 Filer ID:** 838058
- **Principal Place of Business:** 3250 NE 1st Ave Unit 305, Miami, FL 33137, United States
- **Compliance Officer:** compliance@quantumcom.tech
- **Services Provided:** Quantum offers interconnected Voice over IP (VoIP) services, wholesale SIP trunking, enterprise-grade PBX hosting, and call center enablement solutions. Our operations include both retail customer traffic and wholesale carrier interconnections, but all customers are subject to strict compliance and AUP (Acceptable Use Policy) requirements.
- **Operating Model:** Quantum interconnects with multiple Tier-1 carriers and international partners for termination, while maintaining full STIR/SHAKEN implementation across IP-based routes.

- Mission Statement on Robocall Mitigation:

"Quantum is committed to zero tolerance for unlawful robocalls. Our mission is to provide reliable voice communications services that are both innovative and trustworthy, while protecting the public and our partners from abusive traffic."

3. Regulatory Framework:

Quantum's RMP is designed to comply with and reflect the following regulatory obligations and industry standards:

- **FCC Report & Order 20-136:** Establishes requirements for voice providers to implement STIR/SHAKEN or adopt mitigation practices for unauthenticated traffic.
- **47 CFR § 64.6305:** Details obligations for filing RMPs in the FCC's Robocall Mitigation Database.
- **TRACED Act:** Expands the FCC's enforcement authority against robocalls.
- **Truth in Caller ID Act (47 U.S.C. § 227(e)):** Prohibits misleading or inaccurate caller ID information with intent to defraud, cause harm, or wrongfully obtain value.
- **Telephone Consumer Protection Act (TCPA):** Restricts use of autodialers, prerecorded messages, and unsolicited telemarketing without consent.
- **Industry Traceback Group (ITG) Best Practices:** Requires rapid,



Robocall Mitigation Plan (RMP)

Quantum Com LLC

August 2025

accurate responses to traceback requests.

- **STIR/SHAKEN Governance:** As defined by the Secure Telephone Identity Policy Administrator (STI-PA) and Certification Authorities (STI-CAs).
- Quantum has incorporated these obligations into its operational policies and holds itself accountable for continuous compliance.

4. STIR/SHAKEN Implementation

- Deployment Scope

Quantum has fully implemented STIR/SHAKEN on all SIP interconnections where technically feasible. Calls originated within our network are signed with the appropriate attestation level, and inbound calls are verified before routing downstream.

- Attestation Policy

Full Attestation (A): Assigned when Quantum has a direct customer relationship, has validated customer identity, and has verified authority over the calling number.

Partial Attestation (B): Assigned when Quantum has verified the customer identity but cannot fully confirm authority over the number.

Gateway Attestation (C): Assigned when calls originate from an unauthenticated partner with insufficient number ownership validation.

- Certificate Management:

Quantum maintains STI certificates issued by accredited Certification Authorities.

Certificates are stored in secure & backed environments and rotated regularly.

- Interoperability and Verification:

Inbound calls are validated using trusted root certificates. Failed verifications are logged, scored, and may be blocked or quarantined depending on severity.

5. Customer Vetting and Onboarding (KYC/KYB)

- Required Documentation

Before service activation, Quantum requires:

- ⇒ Articles of Incorporation or Business License
- ⇒ Tax Identification Number (EIN)
- ⇒ Government-issued ID for beneficial owners
- ⇒ Corporate officer authorization
- ⇒ Proof of address and operational domain-based email
- ⇒ Evidence of number ownership or assignment (for CLI presentation)

- Screening

All applicants are screened against:

- ⇒ FCC 499-A filer database
- ⇒ Industry complaint registries



Robocall Mitigation Plan (RMP)

Quantum Com LLC

August 2025

- ⇒ Reputation intelligence databases
- **Risk Classification**
 - Reputation Feeds: Integration with industry blacklists and robocall databases.

- ⇒ **Low Risk:** Established enterprises with clean records.
 - ⇒ **Medium Risk:** New companies or moderate call volumes, subject to 90-day enhanced monitoring.
 - ⇒ **High Risk:** Entities with prior complaints, opaque business models, or unverifiable identities — rejected.
- Automated Blocking:
- High-confidence detections are automatically blocked.
 - Suspicious but inconclusive traffic is quarantined and escalated for manual review.

- **Contractual Safeguards**

7. Traceback Cooperation and Law Enforcement

All customers must sign an Acceptable Use Policy (AUP) that prohibits:

Quantum is a proactive member of the Industry Traceback Group (ITG).

- ⇒ Spoofed or fraudulent caller ID
 - ⇒ Autodialed or prerecorded calls without consent
 - ⇒ Calling numbers on the Do Not Call Registry
 - ⇒ Bypassing monitoring systems
- All traceback requests are answered within 24 hours.
 - Complete call origination details are provided, including customer ID and trunk group.
 - Non-cooperative customers are immediately suspended pending review.

6. Real-Time Traffic Monitoring

Quantum employs multi-layered monitoring for call traffic:

Quantum also responds promptly to lawful requests from:

- Call Detail Record (CDR) Analysis: Daily statistical review for ASR, ACD, CPS, and call duration anomalies.
 - Pattern Recognition: Detection of sequential dialing, high-volume short-duration calls, and anomalous geo-distribution.
- FCC Enforcement Bureau
 - Federal Trade Commission (FTC)
 - Other authorized bodies

8. Enforcement and Sanctions

- Graduated Response:



Robocall Mitigation Plan (RMP)

Quantum Com LLC

August 2025

- **Advisory Notice:** Initial anomalies are flagged and the customer is notified.
- **Restrictions:** Rate limits or destination restrictions applied.
- **Suspension:** Temporary service suspension pending investigation.
- **Termination:** Permanent account closure for confirmed violations.

Quantum reserves the right to immediately terminate customers engaged in willful illegal robocalling without prior notice.

9. Data Retention and Security

- CDRs: Retained for 24 months
- Authentication/Verification Logs: 24 months
- KYC Records: 5 years post-termination
- Traceback Responses: 2 years

All data is stored in encrypted databases with strict access controls and audit trails.

10. Employee Training

- New Hire Training: Robocall compliance and STIR/SHAKEN overview
- Quarterly Refreshers: Updates on regulations and threats
- Scenario Drills: Incident simulations for NOC and compliance staff
- Certification: Training completion required for continued system access

11. Governance and Continuous Improvement

- Monthly RMP Review: Updates reflecting FCC rule changes
- Quarterly Independent Audit: External verification of compliance practices
- Board Oversight: Weekly reporting to executive leadership

12. Public Commitment

Quantum publishes a plain-language statement on its website affirming:

- Our zero-tolerance stance on robocalls
- Consumer education resources
- Contact points for reporting abuse