

Meratalk, LLC.

Robocall Mitigation Program & STIR/SHAKEN Implementation

Meratalk, LLC. is a voice service provider ("VSP") based in the **United States**. In accordance with the Federal Communications Commission (FCC) guidelines, specifically the *Sixth Report and Order* (WC Docket No. 17-97), Meratalk has implemented this Robocall Mitigation Program (RMP) to ensure the integrity of its voice traffic and compliance with federal regulations.

1. Executive Summary & Governance

Meratalk is dedicated to preventing illegal calls from originating on our network and monitoring inbound traffic. We leverage advanced infrastructure with full STIR/SHAKEN implementation to enhance mitigation efforts.

- **Zero-Tolerance Policy:** Meratalk enforces a strict policy against illegal robocalling, spoofing, and abusive practices.
- **Compliance Oversight:** Meratalk designates a management-level contact to oversee RMD filings, customer onboarding, and traceback coordination. Policies are documented and updated per regulatory changes.

2. Robocall Mitigation & Traceback

In compliance with FCC requirements, Meratalk adheres to several affirmative obligations to prevent the origination of illegal robocall traffic:

- **Traceback Cooperation:** Meratalk commits to responding fully and within **twenty-four (24) hours** to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium.
- **Investigation Process:** Meratalk cooperates with these entities in investigating and stopping any illegal robocallers that use its service to originate calls.
- **Traceback Contact:**
 - **Name:** NOC Support
 - **Title:** NOC Management
 - **Contact Details:** +1 914-449-5889, noc@meratalk.com.

3. Call Authentication (STIR/SHAKEN)

Meratalk ensures that all traffic is authenticated to provide transparency and traceability:

- **Incoming Traffic:** Our vendors have fully implemented STIR/SHAKEN to sign calls with full attestation and secure call identity.
- **Outbound Traffic:** Underlying long-distance carriers have implemented STIR/SHAKEN and sign Meratalk's calls with **A and/or B attestation**, making calls traceable back to the source in the event of abuse.

4. Advanced Network Monitoring & Traffic Controls

Meratalk utilizes a multi-layered approach to monitor traffic for behaviors consistent with illegal robocalling:

- **Pattern Detection:** Real-time analysis identifies anomalies like sudden spikes or suspicious calling patterns.
- **Blocking Mechanisms:** Meratalk is able to immediately block any calls originating within its network that are identified as illegal robocalls.
- **DNO & Cease-and-Desist:** Meratalk coordinates with industry groups to block government impersonation calls and "call back" DIDs used in scams. We maintain readiness to conduct network-level blocking in response to FCC "cease-and-desist" letters.
- **Proprietary Fraudcheck System:** This system allows the Company to:
 - Prevent users from calling too many numbers in a specific timeframe.
 - Block lines, DIDs, or users suspected of being hacked or originating illegal traffic.
 - Record fraudulent events to prevent future occurrences and notify affected customers.

5. Know Your Customer (KYC) & Risk Assessment

To prevent the use of its network for illegal activities, Meratalk exercises due diligence during the onboarding of new or renewing customers:

- **Identity Verification:** Collecting physical business location, contact person(s), state or county of incorporation, federal tax ID, and the general nature of the business.
- **Risk Classification:** Customers may be categorized based on traffic profiles, with high-risk entities requiring enhanced due diligence.
- **Ongoing Monitoring:** Renewing customers face periodic re-verification to ensure continued compliance.