

ROBOCALL MITIGATION PROGRAM (RMP) DESCRIPTION

VOICE SERVICE PROVIDER CERTIFICATION

Provider Name: Fulton Solutions LLC
FCC FRN: 0038783924
Filing Status: Reseller / Voice Service Provider with No STIR/SHAKEN Implementation Obligation
Target Market: Standard Commercial Office and Professional Service End-Users
Primary Upstream Wholesale Provider: VoIP.ms (BALANCED ROUTING AND COMMUNICATION INC.)

\---

1\. PURPOSE AND NETWORK OVERVIEW

Fulton Solutions LLC operates as a non-facilities-based Voice Service Provider (VSP) reselling Voice over IP (VoIP) services. Our organization caters exclusively to standard commercial business office environments (e.g., professional services, retail offices, local clinics, and corporate enterprises). We explicitly do not market to, onboard, or support high-volume call centers, auto-dialer platforms, telemarketers, or traffic aggregators.

Because we operate as a reseller utilizing the upstream network infrastructure, switching platforms, and telephone number resources of **VoIP.ms**, we do not directly manage cryptographic STIR/SHAKEN token certificates. Instead, we execute a rigorous, localized Robocall Mitigation Program at the customer onboarding and account management layer to completely prevent the origination of illegal, spoofed, or deceptive robocalls.

2\. "KNOW YOUR CUSTOMER" (KYC) ONBOARDING PROTOCOLS

To prevent bad actors from accessing the public switched telephone network (PSTN), we enforce a strict gateway vetting protocol for all new business accounts before provisioning outbound calling privileges:

* **Identity Verification:** We collect and verify official business documentation, including state corporate registry filings (Articles of Organization/Incorporation), Federal Employer Identification Numbers (EIN), and physical commercial address verification via utility bills or lease agreements.

* **Use-Case Evaluation:** Every prospective customer must complete a usage profile. We verify that their calling habits conform to normal business office operations (e.g., traditional seat-based business lines with human-initiated dialing). Any entity intending to run automated notifications, pre-recorded messages, or high-density outbound campaigns is denied service.

* **Authorized Number Restrictions:** Customers are prohibited from inputting unverified Caller IDs. Outbound Caller IDs are strictly locked to the Direct Inward Dialing (DID) numbers legitimately assigned to the

customer through our partner portal or verified via a formal Letter of Authorization (LOA) porting process.

3\ . TRAFFIC MONITORING AND SPOOFING PREVENTION

In tandem with the upstream analytics provided by our wholesale network partner, we monitor account behaviors to detect patterns indicating a compromised system or policy breach:

- * **Anomaly Baselines:** Because our clientele consists solely of standard offices, we establish strict mathematical baselines for normal business traffic. We monitor for sudden spikes in call volume, unusually high ratios of short-duration calls (under 6 seconds), and high volumes of unanswered or concurrent calls.
- * **Proactive Blocking:** Our routing profiles reject calls that attempt to broadcast invalid, unallocated, or restricted numbers (such as spoofed 911, 000-000-0000, or premium-rate prefixes).
- * **Credential Security:** To prevent SIP registration hijacking (which bad actors use to blast automated calls), we mandate complex, randomly generated alphanumeric SIP passwords and restrict device registrations to verified IP ranges wherever technically feasible.

4\ . MANDATORY TRACEBACK COOPERATION

Fulton Solutions LLC maintains full accountability for all traffic originating from our clients and fully cooperates with all regulatory and industry investigative bodies:

- * **24-Hour Service Level Agreement (SLA):** We commit to responding to all official traceback requests from the Federal Communications Commission (FCC), the Industry Traceback Group (ITG), and law enforcement agencies within 24 hours of receipt.
- * **Audit Trail Investigation:** Upon receiving an ITG traceback alert, our engineering team will cross-reference the flagged Call Detail Records (CDRs) against our client billing database to immediately identify the exact sub-customer account that initiated the traffic.
- * **Upstream Escalation:** We maintain open compliance lines with our upstream provider, VoIP.ms, to assist them in tracebacks or network investigations involving our blocks of telephone numbers.

5\ . STRICT ENFORCEMENT AND DISCONNECTION POLICIES

We maintain a zero-tolerance policy for network abuse. Our master service agreements contain clear provisions allowing for immediate disciplinary actions:

- * **Immediate Suspension:** If an investigation or real-time monitoring reveals that a customer is originating unauthorized automated robocalls, illegal telemarketing, or deceptive spoofed traffic, we reserve the right to instantly suspend their SIP trunks and terminate outbound calling capabilities without prior notice.
- * **Upstream Reporting \& Permanent Termination:** Customers found in intentional violation of federal robocall mandates are permanently banned from our platform. If the traffic is deemed criminal, we will proactively

report the client identity and data logs to our wholesale partner and appropriate law enforcement entities.

\---

****EXECUTIVE CERTIFICATION:****

By submitting this program description to the FCC Robocall Mitigation Database, the authorized corporate officer of the company certifies under penalty of perjury that the practices detailed above are fully implemented, monitored, and maintained as the company's official operating protocol.