

# **Send buddy**

## **Robocall Mitigation Plan**

*FCC Compliance Submission Under 47 C.F.R. § 64.6305*

### **I. Provider Overview**

---

ATTACK ON TITAN (DBA as Sendbuddy) is an interconnected VoIP provider specializing in international gateway traffic collection. This document sets forth Sendbuddy's Robocall Mitigation Program (RMP), encompassing the following key components:

- Implementation of STIR/SHAKEN call authentication in accordance with the FCC's extension provisions for small providers.
- Proactive practices to prevent, detect, and mitigate illegal robocalls originating from or traversing the Sendbuddy network.

Commitment: Sendbuddy is fully committed to compliance with all applicable FCC regulations and industry best practices. The company cooperates proactively with traceback requests and actively supports industry-wide efforts to combat illegal robocall activity.

### **II. Mitigation Measures**

---

#### **1. Customer Compliance & Enforcement**

All Sendbuddy customers are contractually required to adhere to the following:

- Full compliance with FCC, FTC, TCPA, and all applicable state and federal anti-robocall laws and regulations.
- Acknowledgment of termination clauses, which authorize Sendbuddy to suspend or permanently terminate services upon confirmed violations of applicable laws or Sendbuddy policies.

#### **2. Know Your Customer (KYC) Policy**

Sendbuddy maintains a rigorous Know Your Customer (KYC) framework applicable to all wholesale, enterprise, and call center customers. Key components include:

##### **Onboarding Verification:**

- Collection and verification of business address, primary contact information, incorporation documentation, Tax Identification Number (Tax ID), USAC ID, and banking details.
- Assessment of the nature of each customer's business to identify and evaluate potential robocall risk exposure.

### **3. Network Monitoring & Fraud Prevention**

Sendbuddy employs continuous, real-time traffic analysis to proactively identify and respond to suspicious activity, including:

- Robocalling patterns and high-volume automated traffic anomalies.
- Traffic pumping schemes and international toll fraud indicators.

#### **Enforcement Actions:**

- Immediate blocking of identified fraudulent or non-compliant traffic.
- Termination of services for customers engaged in intentional illegal robocalling activities.

### **4. Carrier Vetting & Traffic Acceptance**

Sendbuddy enforces strict criteria for the acceptance of termination traffic. Traffic is accepted exclusively from carriers that:

- Are listed and in good standing in the FCC Robocall Mitigation Database.
- Demonstrate compliance with STIR/SHAKEN call authentication standards and all applicable anti-robocall policies.

### **5. Traceback Cooperation**

Sendbuddy maintains a 24/7 operational posture to support traceback investigations, including:

- Prompt cooperation with the FCC, law enforcement agencies, and recognized traceback consortiums, with responses provided within 24 hours of a request.
- Full investigative assistance to identify, isolate, and halt illegal robocall traffic traversing the Sendbuddy network.

## **III. STIR/SHAKEN Implementation**

---

#### **Current Status:**

- Sendbuddy is actively deploying STIR/SHAKEN call authentication technology across its IP network infrastructure, in accordance with the FCC's small provider extension provisions.

#### **Future Commitments:**

- Ongoing infrastructure upgrades to achieve full compliance with FCC-mandated STIR/SHAKEN deadlines.
- Strategic partnerships with certified analytics providers to enhance call authentication capabilities and fraud detection.

## **IV. Continuous Improvement**

---

**Adaptive Measures:**

- Regular review and updates to the Robocall Mitigation Program to ensure alignment with evolving FCC regulatory requirements and emerging industry best practices.
- Ongoing enhancements to network monitoring tools, KYC verification processes, and enforcement protocols to address new and emerging threats.