

Robocall Mitigation Program Description

Company Name: [MTP Galaxy Co.]

FCC FRN: [0037161429]

Date: June 19, 2025

1. Company Overview

[MTP Galaxy Co.] is a [domestic] VoIP service provider headquartered in [The United States]. We provide voice communication services to enterprise customers, some of whom may originate calls terminating in the United States.

We are not a facilities-based carrier and do not currently have interconnections with the PSTN in the U.S. All of our calls are delivered to U.S. destinations through our upstream carrier partners.

We are currently not fully STIR/SHAKEN-capable, as our calls do not originate on an IP network in the United States. Therefore, we are required to submit this Robocall Mitigation Plan to the FCC in accordance with 47 CFR § 64.6305(c).

2. Robocall Mitigation Practices

[MTP Galaxy Co.] implements a comprehensive robocall mitigation strategy that includes:

- Real-time traffic monitoring to identify anomalies such as high call volumes, short-duration calls, or repetitive calling patterns.
- Automated traffic pattern analysis using software tools to flag potential illegal robocall behavior.
- Call volume caps and rate limiting to detect and restrict suspicious call bursts.
- Use of call reputation services and destination number analysis to block known bad traffic.

Our network is monitored 24/7 using our self-developed reputation scoring and call analytics services. For every call originated on our platform, a real-time query is made to this service. Calls that receive a high-risk score, utilize a telephone number present on a Do-Not-Originate (DNO) list, or exhibit patterns consistent with illegal robocalling (e.g., excessive calls-per-second, extremely low answer-seizure ratio) are automatically blocked before leaving our platform. Our compliance team reviews blocked call reports daily to identify and investigate potential bad actors.

We have implemented a strict telephone number validation process. Customers may only use telephone numbers as their Caller ID if they provide proof of ownership or a Letter of Authorization (LOA) from the number's subscriber of record. All authorized numbers for a customer are maintained in a 'whitelist' within our system, and any attempt to originate a call using a non-whitelisted number is automatically rejected. Furthermore, we periodically check customer numbers against the Reassigned Numbers Database (RND) to prevent the use of disconnected numbers.

3. Customer Vetting Procedures

We apply strict Know Your Customer (KYC) procedures prior to onboarding any customer, which include:

- Collecting government-issued business registration documents
- Verifying customer identification and business purpose
- Evaluating the legitimacy of customer use cases for outbound calling
- Requiring attestation that the customer will not use the service to originate illegal robocalls

As a mandatory part of our customer onboarding process, we collect and verify the following information for every client: legal business name, physical business address (P.O. Boxes are not accepted), state/country of incorporation records, and the full name, title, and direct contact information for a responsible officer of the company. For customers engaged in marketing activities, we require a written description of their process for obtaining consumer consent in compliance with the TCPA and TSR. We reserve the right to refuse service to any applicant that fails to provide satisfactory information.

Customers found violating our acceptable use policy are immediately suspended and investigated.

4. Complaint Handling & Traceback Cooperation

We maintain a designated compliance contact to receive and respond to robocall complaints:

Compliance Contact: [Yingyang Xiong], [Director]
Email: [business_development@jekka.ai]
Phone: [+1 (213) 207-0665]

We commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers that use our services. The

designated point of contact for all such requests is listed in our RMD filing. We maintain call detail records (CDRs) for a minimum of 12 months for audit and investigation purposes.

5. Recordkeeping and Auditing

We retain detailed CDR logs for all calls passing through our platform, including:

- Originating number
- Destination number
- Timestamp
- Call duration
- Customer identifier

Regular audits are conducted on high-risk traffic, and alerts are generated for abnormal calling behavior.

6. Acceptable Use Policy

Our customer agreements incorporate by reference a binding Acceptable Use Policy (AUP), which explicitly prohibits the use of our services for originating any illegal, abusive, or fraudulent calls, including but not limited to violations of the TCPA and the Telemarketing Sales Rule (TSR). The AUP grants us the express right to suspend or terminate, without prior notice, any services found to be in violation of this policy in order to prevent harm to our network and the public.

7. Compliance Certification

[MTP Galaxy Co.] certifies that it has implemented the robocall mitigation practices described above to the best of its ability and will continue to enhance its detection and enforcement methods in accordance with FCC rules.

Signed,

[Yingyang Xiong]

[Director]

[MTP Galaxy Co.]

[business_development@jekka.ai]

Date: June 19, 2025