



Katko Networks LLC

ROBOCALL MITIGATION PLAN

September 2026

Table of Contents

Table of Contents.....	2
1. Purpose and Scope.....	3
2. Company Summary.....	3
3. Certifications.....	3
4. Call Authentication — STIR/SHAKEN.....	3
5. Know Your Customer (KYC).....	4
6. Know Your Upstream Provider (KYUP).....	5
7. Traffic Acceptance — RMD-Listed Providers Only.....	5
8. Network Monitoring, Analytics, and Call Blocking.....	5
9. Mandatory Blocking Following Commission Notification.....	6
10. Traceback Cooperation.....	6
11. Emergency Call and Do-Not-Originate Protections.....	6
12. Contractual Framework.....	6
13. Caller ID Integrity.....	7
14. Training and Awareness.....	7

1. Purpose and Scope

This Robocall Mitigation Plan (“Plan” or “RMP”) describes the policies, procedures, and technical and contractual controls maintained by Katko Networks LLC (“Katko” or the “Company”) to prevent the origination and transmission of illegal robocall traffic on its network. This Plan is intended to satisfy Katko’s robocall mitigation and certification obligations under 47 C.F.R. § 64.6305.

This Plan is reviewed periodically and updated as necessary to reflect changes in Katko’s operations, network architecture, vendor relationships, or applicable FCC requirements.

2. Company Summary

Legal Name	Katko Networks LLC
Federal EIN	38-4348919
Business Purpose	Wholesale telecommunications — VoIP voice and SMS messaging services
Principal:	Valtteri Serimaa (Owner/CEO)
Principal Address	8 The Green, STE B, Dover, DE 19901
Main Telephone	651-802-0409
Website	https://katkonetworksllc.com

3. Certifications

In connection with this Plan and its RMD submission, Katko Networks LLC affirms the following:

- Katko has implemented, and complies with, the robocall mitigation practices described in this Plan, which are reasonably designed to significantly reduce the transmission of illegal robocall traffic.
- No prior robocall mitigation certification of Katko has been removed by Commission action, and Katko is not otherwise prohibited from filing in the RMD.
- The information provided in this Plan and in the associated RMD certification is true, accurate, and complete to the best of Katko’s knowledge, and the individual submitting the certification is authorized to do so on behalf of the Company.
- Katko will update its RMD filing within 10 business days of any change to the information submitted, as required by 47 C.F.R. § 64.6305(d)(5), and will complete the required annual recertification.
- Katko will recertify annually, on or before March 1, that the information in its RMD filing remains true and correct, consistent with 47 C.F.R. § 64.6305(h).

4. Call Authentication — STIR/SHAKEN

Katko operates as a wholesale originating voice service provider and is currently completing implementation of the STIR/SHAKEN caller ID authentication framework. Pending full implementation,

Katko applies the robocall mitigation measures described in this Plan to traffic for which it acts as the originating provider. Katko expects to complete implementation after obtaining its Operating Company Number and completing the necessary registration, certification, and technical steps. Katko will update its RMD filing within 10 business days of any change in its implementation status.

5. Know Your Customer (KYC)

Katko applies documented Know Your Customer procedures to every customer before provisioning service and on an ongoing basis thereafter. The objective is to verify each customer's identity, legitimacy, regulatory standing, and intended use of service, and to deny or terminate service where the risk of illegal traffic is unacceptable.

5.1 Onboarding Due Diligence

Prior to executing a service agreement, Katko collects and verifies the following from each prospective customer:

- Legal business name, entity type, physical business address, and main telephone number.
- Type of business and the categories of voice/messaging services the customer provides.
- Key personnel contact details (name, title, email, telephone, and where available LinkedIn profile).
- FCC Registration Number (FRN) and FCC Form 499 Filer ID, where applicable.
- Federal Tax ID (FEIN) or foreign equivalent.
- RMD registration status and Operating Company Number (OCN), where applicable.
- Regulatory profile: whether the customer originates calls, acts as a gateway for foreign-originated traffic, engages in telemarketing, has implemented STIR/SHAKEN, and maintains its own robocall mitigation plan.
- Whether the customer has been designated a non-cooperative voice service provider by the ITG or is subject to any FCC enforcement action.

5.2 Validation

Katko validates the information provided by cross-checking independent sources, including: the customer's website and public/social presence; confirmation of FCC Form 499 and FRN records; verification of RMD listing (and that it is not de-listed); consistency of the customer's stated business with the data filed in the RMD; etc. Katko reserves the right to request additional documentation at any time as a condition of onboarding or continued service.

Katko maintains records of its completed KYC reviews and supporting verification materials for compliance and risk-management purposes.

5.3 Ongoing Review

Katko refreshes KYC information for active customers on a recurring basis and upon any material change, trigger event, or elevated-risk indicator identified through traffic monitoring. Continuation of service is conditioned on the customer's timely and complete cooperation with these requirements.

6. Know Your Upstream Provider (KYUP)

Katko maintains know-your-upstream-provider procedures consistent with 47 C.F.R. § 64.1200(n)(5) and § 64.6305(d)(2)(ii). Before accepting traffic from an upstream provider, Katko:

- Confirms the upstream provider is listed in the RMD and that the listing has not been de-listed, before accepting traffic directly from that provider.
- Records the identity, contact information, and regulatory identifiers (FRN, 499 Filer ID, OCN, RMD status) of each upstream provider.
- Requires contractual commitments from upstream providers to comply with applicable robocall and caller ID authentication rules and to cooperate with traceback.
- Monitors the quality and legitimacy of traffic received from each upstream provider and escalates, restricts, or terminates the relationship where illegal or abusive traffic is identified.

7. Traffic Acceptance — RMD-Listed Providers Only

Consistent with 47 C.F.R. § 64.6305(g), Katko accepts calls directly from another provider only where that provider's filing appears in the RMD. Katko maintains procedures to confirm RMD status at onboarding and to periodically re-verify that upstream and peer providers remain listed.

8. Network Monitoring, Analytics, and Call Blocking

Katko monitors traffic across its network on a continuous basis and uses its own analytics platform, supported by internal review, to detect and act on patterns indicative of illegal robocalling. Monitoring and enforcement include:

- Detection of abnormal traffic patterns through calls-per-second/session limits and anomaly detection.
- Analysis of key metrics such as answer-seizure ratio (ASR), average call duration and short-duration calling, invalid or unassigned ANIs, and excessive call-failure rates.
- Application of a Do-Not-Originate (DNO) filter to block calls purporting to originate from numbers that should never originate calls.
- Blocking of media/source IPs associated with suspicious or unlawful campaigns, or reported through FCC, carrier, or CLEC complaints.
- Reputation and reported-scam screening to identify and block high-risk sources.
- Where Katko blocks calls based on reasonable analytics and the applicable FCC signalling requirements apply, Katko uses SIP response code 603+ in accordance with 47 C.F.R. § 64.1200(k)(9).

Katko monitors traffic using automated controls and periodic internal review, as appropriate to its network operations. When illegal robocalling or caller ID spoofing is suspected, Katko promptly identifies the responsible party and takes timely action, including suspension or blocking of the offending traffic. Calls carrying valid STIR/SHAKEN signatures are passed unaltered.

9. Mandatory Blocking Following Commission Notification

Upon receipt of a Notice of Suspected Illegal Traffic from the FCC's Enforcement Bureau, Katko will promptly and diligently investigate the identified traffic. Where Katko's investigation confirms that the traffic is illegal or where the Commission directs blocking, Katko will block the identified traffic and will take reasonable steps to identify and cease accepting traffic from the responsible upstream source. Katko will report the results of its investigation to the Commission as required.

10. Traceback Cooperation

Katko participates in the industry traceback process and complies with the 24-hour traceback response obligation under 47 C.F.R. § 64.6305(c)(2). Specifically, Katko:

- **24-hour response.** Responds fully within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium (ITG), and cooperates in investigating and stopping illegal robocallers that use its service to carry or process illegal traffic.
- **Secure portal.** Uses the ITG secure traceback portal to review and confirm traffic records and to identify the upstream source of flagged traffic.
- **Dedicated point of contact.** Maintains a designated point of contact responsible for receiving and actioning traceback and suspicious-traffic requests.

Name	Valtteri Serimaa
Title	CEO
Telephone	651-802-0409
Email	compliance@katkonetworksllc.com

- **Ongoing coordination.** Exchanges information regarding suspicious traffic with other providers and industry bodies to support timely mitigation.

11. Emergency Call and Do-Not-Originate Protections

Katko does not block calls to 911 unless it knows without a doubt that the call is unlawful. Katko also makes all reasonable efforts to avoid blocking calls from Public Safety Answering Points and government outbound emergency numbers, consistent with 47 C.F.R. § 64.1200(k)(5)-(6).

12. Contractual Framework

Each Katko customer must execute a Master Service Agreement (MSA) and comply with all applicable federal, state, and international laws and regulations governing telecommunications services, including those related to robocalls, caller ID authentication, and consumer protection. Katko's Acceptable Use Policy (AUP) prohibits use of its services for any unlawful, fraudulent, abusive, or deceptive activity, including the origination or transmission of illegal robocalls and caller ID spoofing.

Under its MSA and AUP, Katko reserves the right to suspend, restrict, or terminate service, in whole or in part, immediately and without prior notice where Katko reasonably determines such action is necessary due to an AUP violation, suspected or actual fraud, a regulatory or legal compliance obligation (including FCC requirements), or to protect the integrity of its network, its customers, or third parties.

13. Caller ID Integrity

Katko does not knowingly permit the use of its services to transmit unlawful spoofed caller ID information. Where Katko identifies suspected caller ID misuse, it evaluates the circumstances and takes appropriate action consistent with applicable law, FCC requirements, and its contractual rights. This may include requesting additional information, restricting traffic, suspending service, or terminating the customer relationship.

14. Training and Awareness

Katko provides ongoing training to its commercial and technical personnel on robocall mitigation policies and procedures. Training covers applicable FCC requirements, identification of suspicious traffic patterns, KYC and KYUP protocols, traceback obligations, and internal escalation procedures, so that staff responsible for onboarding, routing, and monitoring are equipped to prevent, detect, and respond to illegal robocall activity.