



ROBOCALL MITIGATION PLAN

October 2026

Table of Contents

1. Purpose and Applicability	3
2. Company Profile	3
3. Caller ID Authentication — STIR/SHAKEN	4
4. Customer Due Diligence (KYC)	4
5. Upstream Provider Due Diligence (KYUP)	5
6. Accepting Traffic Only from RMD-Listed Providers	5
7. Traffic Monitoring, Analytics and Blocking	5
8. Blocking Required by FCC Notice	6
19. Traceback Support	6
10. Customer Agreements and Acceptable Use	7

1. Purpose and Applicability

KSwap Networks LLC (“KSwap” or the “Company”) has adopted and implements this Robocall Mitigation Plan (the “Plan”) to establish the operational, technical and contractual measures it uses to prevent illegal robocalls from being originated on or carried across its network. KSwap will operate as a wholesale originating voice service provider, gateway provider and intermediate provider, depending on its role in the call path. The Company will apply the regulatory requirements and robocall mitigation practices applicable to the role it performs for each call.

These measures are reasonably designed to substantially reduce illegal robocall traffic and support the Company’s robocall mitigation and certification obligations under 47 C.F.R. § 64.6305. In connection with this Plan and its Robocall Mitigation Database (“RMD”) filing, KSwap certifies that it follows the mitigation practices described herein; that the Commission has never removed a robocall mitigation certification filed by KSwap; and that nothing prevents the Company from filing in the RMD. To the best of KSwap’s knowledge, this Plan and its related RMD certification are true, accurate and complete.

KSwap regularly reviews this Plan and revises it whenever its operations, network design, vendors or applicable FCC requirements change. The Company will update its RMD filing within ten business days of any change to the information on file and will recertify annually, no later than March 1, that its filing remains true and correct, in accordance with 47 C.F.R. § 64.6305.

2. Company Profile

Legal Name	KSwap Networks LLC
Federal EIN	35-2986837
State of Formation	Delaware (File No. 10781008)
Business Purpose	Wholesale telecommunications — VoIP voice termination, SMS/A2P messaging, DID numbers and carrier interconnection services
Principal	Adriana M. Rangel Rojas (Manager)
Principal Address	254 Chapman Rd, Ste 208 #28833, Newark, DE 19702
Main Telephone	+1 (302) 302-1652
Website	https://www.kswapnet.com

3. Caller ID Authentication — STIR/SHAKEN

KSwap is in the process of obtaining an Operating Company Number (OCN) and completing the steps necessary to implement STIR/SHAKEN. Once implementation is complete, the Company will fully comply with the STIR/SHAKEN requirements applicable to its operations.

4. Customer Due Diligence (KYC)

Every customer goes through KSwap's documented Know Your Customer (KYC) process before any service is activated and remains subject to it for as long as the relationship lasts. The process confirms who the customer is, that its business is legitimate, its regulatory standing, and how it intends to use the service. KSwap declines or ends service whenever the risk of illegal traffic is too high.

4.1 Information Collected at Onboarding

Before a service agreement is signed, each prospective customer must provide, and KSwap verifies:

- Its full legal name, type of entity, physical business address and main phone number.
- A description of its business and of the voice and messaging services it offers.
- Contact details for key personnel, including name, title, email, phone number and, where available, LinkedIn profile.
- Its FCC Registration Number (FRN) and FCC Form 499 Filer ID, if applicable.
- Its U.S. Federal Employer Identification Number (FEIN) or the foreign equivalent.
- Its RMD filing status and Operating Company Number (OCN), if applicable.
- Its regulatory profile, including whether it originates calls, serves as a gateway for traffic originating abroad, conducts telemarketing, has deployed STIR/SHAKEN and has its own robocall mitigation plan.
- Whether the Industry Traceback Group (ITG) has designated it a non-cooperative voice service provider, or whether it is the subject of any FCC enforcement action.

4.2 Verification

KSwap verifies customer information against independent sources, including the customer's website, public and social media presence, FCC Form 499 and FRN records, and the RMD, confirming that the customer is listed and has not been removed. The Company also checks that the customer's stated business activities are consistent with its RMD filing.

KYC information for active customers is refreshed periodically and whenever a material change, triggering event or heightened-risk signal identified through traffic monitoring warrants further review. KSwap may request additional documentation as a condition of onboarding or continued service, and customers must cooperate fully and promptly with these reviews.

Records of each initial and subsequent KYC review, together with supporting evidence, are retained for compliance and risk-management purposes.

5. Upstream Provider Due Diligence (KYUP)

KSwap applies know-your-upstream-provider procedures consistent with 47 C.F.R. § 64.1200(n)(5) and describes these procedures pursuant to § 64.6305(d)(2)(ii), (e)(2)(ii) and (f)(2)(ii), as applicable to its role in the call path.

Before accepting traffic directly from an upstream provider, KSwap:

- Verifies that the provider is listed in the RMD and is not subject to an FCC removal or blocking order that prohibits acceptance of its traffic.
- Records and verifies the provider's identity, contact details and regulatory identifiers, including its FRN, Form 499 Filer ID, OCN and RMD identification, as applicable.
- Obtains contractual commitments to comply with applicable robocall mitigation and caller ID authentication requirements and to cooperate fully with traceback requests.

Throughout the relationship, KSwap periodically rechecks the provider's RMD status, reviews relevant FCC enforcement developments and monitors the traffic it delivers for indications of illegal calling. Concerns trigger further investigation and appropriate action, which may include traffic restrictions, blocking, suspension or termination

6. Accepting Traffic Only from RMD-Listed Providers

In line with 47 C.F.R. § 64.6305(g), KSwap takes calls directly from another provider only if that provider has a filing in the RMD. KSwap checks RMD status when a provider is onboard and re-checks it periodically to confirm that upstream and peer providers are still listed.

7. Traffic Monitoring, Analytics and Blocking

KSwap continuously monitors traffic on its network using its own analytics platform and internal review to identify and respond to patterns that may indicate illegal robocalling. Its monitoring and enforcement tools include:

- Calls-per-second and concurrent-session limits, together with anomaly detection, to flag unusual traffic patterns.
- Review of key indicators, including answer-seizure ratio (ASR), average call duration, high volumes of short-duration calls, invalid or unassigned ANIs and unusually high call-failure rates.

- A Do-Not-Originate (DNO) filter that blocks calls appearing to originate from numbers that should never originate calls.
- Blocking of source IP addresses and media endpoints associated with suspicious or unlawful campaigns, including those identified through FCC notifications or carrier complaints.
- Reputation and reported-scam screening to identify and block high-risk traffic sources.
- Use of SIP response code 603+ when KSwap blocks calls based on reasonable analytics and applicable FCC signaling requirements apply. KSwap also transmits downstream SIP 603+ responses toward the call's origination point, consistent with 47 C.F.R. § 64.1200(k)(9).

These controls combine automated tools with periodic internal review, scaled to KSwap's network operations. When illegal robocalling or caller ID spoofing is suspected, KSwap promptly investigates, identifies the responsible party and takes appropriate action, including restricting, suspending or blocking the affected traffic.

KSwap preserves STIR/SHAKEN authentication information when forwarding calls. Authenticated calls remain subject to the monitoring and blocking controls described in this Plan.

KSwap applies its monitoring, DNO and blocking controls with safeguards for emergency communications. KSwap will not block emergency calls placed to 911 and will make all reasonable efforts to avoid blocking calls from Public Safety Answering Points or government emergency numbers, consistent with 47 C.F.R. §§ 64.1200(k)(5)–(6) and 64.6305(g)(5).

8. Blocking Required by FCC Notice

KSwap will promptly investigate traffic identified in an FCC Enforcement Bureau notice, report its findings and take the mitigation or blocking actions required for its role in the call path within the applicable deadlines, consistent with 47 C.F.R. § 64.1200(n)(2)–(3)

19. Traceback Support

KSwap responds fully within 24 hours to traceback requests from the Commission, law enforcement and the Industry Traceback Group (ITG), consistent with 47 C.F.R. § 64.6305(c)(2), and cooperates in investigating and stopping illegal robocallers using its services. The Company uses the ITG's secure portal to review call records and identify the upstream source of flagged traffic, maintains a designated contact for traceback and suspicious-traffic requests, and coordinates with other providers and industry groups as appropriate.

Name	Adriana M. Rangel Rojas
Title	Manager
Telephone	+1 (302) 302-1652
Email	adriana.rangel@kswapnet.com

10. Customer Agreements and Acceptable Use

All KSwap customers must sign a Master Service Agreement (MSA) and abide by every federal, state and international law and regulation that applies to telecommunications services, including the rules on robocalls, caller ID authentication and consumer protection. KSwap's Acceptable Use Policy (AUP) forbids any use of its services for unlawful, fraudulent, abusive or deceptive purposes, including originating or carrying illegal robocalls and spoofing caller ID.

The MSA and AUP allow KSwap to suspend, limit or terminate service, in whole or in part, immediately and without prior notice, whenever it reasonably concludes that this is needed because of an AUP breach, suspected or actual fraud, a legal or regulatory obligation (including FCC requirements), or to protect its network, its customers or third parties.