

ROBOCALL MITIGATION PLAN

Prepared for K & A Innovations, LLC - FCC Robocall Mitigation Database Filing

Filing entity	K & A Innovations, LLC
DBA / trade name	K & A Innovations, LLC
Business FRN	0037052826
Prepared / revised date	March 24, 2026

1. Purpose and scope

This Robocall Mitigation Plan describes the policies, procedures, technical controls, and escalation steps used by K & A Innovations, LLC (the “Company”) to mitigate illegal robocalls and spoofed traffic in connection with the voice services it originates, carries, processes, or otherwise provides. The Company adopts these measures to meet the Federal Communications Commission’s Robocall Mitigation Database filing requirements and to reduce the likelihood that its network, services, numbering resources, or customer relationships will be used to originate or transmit illegal robocalls.

This plan applies to the Company’s operations, personnel, resellers (if any), contractors, customer onboarding processes, numbering and caller-ID practices, traffic monitoring activities, traceback responses, and enforcement actions for voice services associated with the entity identified in this filing.

2. Company identification and filing profile

Legal name of filer	K & A Innovations, LLC
Current business / trade names	K & A Innovations, LLC
Previous names used within the last two years	None.
Business address	140 Old Gray Station Rd, Suite 200, Gray, TN 37615, United States
Primary website	kainnovations.com
Role in the call path	Voice Service Provider
Foreign voice service provider status	No
Operating Company Number (OCN)	No OCN

The Company provides the following services: white-label hosted voice and related VoIP services to end-user customers using the SkySwitch platform. The Company serves primarily business end users in the United States and uses SkySwitch and its underlying network/platform arrangements in the provision of those services.

3. STIR/SHAKEN implementation status

The Company will make the STIR/SHAKEN certification in the RMD that accurately reflects its network and service environment. The selection below should match the filing exactly.

Item	Company response
Filing selection	Option 3 - No STIR/SHAKEN Implementation
Network description	Reseller / white-label voice service provider environment that relies on the underlying SkySwitch platform and provider-controlled network infrastructure for network-level call authentication where applicable.
SPC token / certificate status	Not applicable based on current operating model; K & A Innovations, LLC does not independently control the SBC/signing environment and does not separately identify its own SPC token or STI certificate for outbound authentication in this filing posture.
Third-party authentication arrangement	Underlying provider arrangement: SkySwitch. K & A Innovations, LLC relies on the underlying platform/provider for network-level STIR/SHAKEN implementation where applicable under its current reseller model.
Applicable exemption or extension	Lack of control over the network infrastructure necessary to implement STIR/SHAKEN under the Company's current white-label reseller model using the SkySwitch platform.

If the Company certifies to partial or no STIR/SHAKEN implementation, the Company will explain in the filing and, if helpful, in this plan why the cited exemption or extension applies. If the Company uses a third party for the technical act of authentication, the Company remains responsible for the accuracy of its filing, its attestation decisions, and any certificate-related obligations that apply to it under FCC rules.

4. Robocall mitigation program

The Company takes reasonable steps that are designed to significantly reduce the origination, carrying, or processing of illegal robocalls. The measures below are intended to work together as a layered control framework, combining customer due diligence, technical safeguards, traffic review, traceback responsiveness, and prompt enforcement.

4.1 Customer onboarding and know-your-customer procedures

Before activating service for a new customer, the Company performs reasonable know-your-customer ("KYC") checks designed to confirm the customer's identity, the legitimacy of the proposed calling activity, and the customer's authority to use any telephone numbers or caller IDs presented through the Company's service.

- Collecting and verifying core account information, including legal business name, trade name, business address, billing information, tax ID or company registration information as appropriate, and the identity of the authorized representative establishing service.
- Documenting the customer's expected use case, traffic profile, target audience, vertical, and whether the customer intends to engage in outbound calling campaigns, prerecorded/artificial voice traffic, or higher-volume activity.
- Reviewing the customer's website, marketing materials, or business presence, and requesting additional information for higher-risk use cases such as lead generation, debt relief, short-duration outbound campaigns, affiliate marketing, political calling, or healthcare-related outreach.

- Obtaining written confirmation that the customer will comply with applicable calling laws and consent requirements, including the Telephone Consumer Protection Act, caller-ID rules, and the Company's acceptable-use policy.
- Applying enhanced review, delayed activation, number restrictions, or a denial of service when customer information is incomplete, inconsistent, unverifiable, or indicative of elevated robocall risk.

For existing customers, the Company revisits KYC information when material changes occur, including ownership changes, unusual traffic shifts, new use cases, or complaints suggesting that the customer's account may be involved in unlawful or abusive calling.

4.2 Upstream provider and partner diligence

The Company also maintains reasonable procedures to know its upstream providers and key voice-service partners. Those procedures may include maintaining a current list of upstream providers, reviewing service agreements and compliance commitments, confirming the provider's current presence in the RMD where applicable, and maintaining operational contacts for compliance and traceback matters.

- Underlying provider(s) and important network partners used by the Company: SkySwitch..
- If the Company relies on an underlying provider for analytics or call treatment, that provider is identified here: SkySwitch (underlying provider), where applicable..
- The Company reviews whether upstream or partner relationships present increased robocall risk and escalates any compliance concerns for management review.

4.3 Numbering, caller ID, and right-to-use controls

The Company uses procedures intended to prevent the use of invalid, unauthorized, or misleading caller ID information. The Company does not knowingly permit customers to use numbers they are not authorized to use or to present caller ID information in a manner that is deceptive or unlawful.

- Only assigning or enabling caller IDs that are purchased through the Company, assigned by an authorized provider, or supported by documentation showing the customer's right to use the number.
- Reviewing and approving bring-your-own-number ("BYON" or "BYOT") requests before those numbers are activated for outbound caller-ID presentation.
- Blocking, disabling, or escalating caller-ID values that appear invalid, unallocated, unassigned, spoofed, inconsistent with account records, or associated with known do-not-originate lists where applicable.
- Restricting or disabling features that would allow unauthorized caller-ID manipulation or high-risk traffic patterns when the Company determines such restrictions are warranted.

4.4 Traffic monitoring, analytics, and anomaly detection

The Company monitors traffic and account behavior for patterns reasonably associated with illegal robocalls or spoofing. Monitoring may be performed through internal review, automated thresholds, third-party analytics, underlying-provider analytics, or a combination of these methods.

Monitoring topic	Company response / description
Uses analytics as part of mitigation program?	Yes - the Company relies on a combination of internal traffic review and underlying-provider monitoring where applicable.
Analytics vendor(s)	SkySwitch (underlying provider) for platform-level monitoring where applicable; internal review of complaints, account activity, and traffic anomalies by Company personnel.
Signals reviewed	Calling spikes after onboarding, unusual calling volumes, suspicious calling

	patterns, complaint activity, repeated caller-ID changes, invalid or unauthorized number use indicators, unusual geographic patterns, and other traffic anomalies identified through account review or underlying-provider monitoring.
Review cadence	Ongoing review through underlying-provider monitoring where applicable, plus complaint-driven and anomaly-driven review by Company personnel during normal business operations with escalation as needed.
Escalation trigger examples	Traffic spikes after onboarding, suspicious outbound campaigns, repeated complaints, invalid or unauthorized caller-ID use, anomalous destinations, sudden volume changes, fraud alerts, or any upstream-provider notice that suggests suspicious traffic.

When the Company identifies suspicious traffic, the Company may place the account under review, limit calling permissions, request additional customer information, block specific caller IDs or destinations, suspend service, or terminate service, depending on the severity of the issue and the evidence available.

4.5 Complaint intake and internal investigation

The Company accepts robocall- and spoofing-related complaints from customers, upstream providers, law enforcement, the registered traceback consortium, and other industry participants. Complaints are routed to Operations / management contact led by Keven Vrotney, COO for review.

- Logging the complaint date, source, affected number(s), account involved, and a summary of the alleged conduct.
- Reviewing call detail records, caller-ID usage, provisioning records, KYC materials, and any prior warnings or complaint history tied to the account or number.
- Escalating credible reports to management and taking interim measures when necessary to reduce ongoing harm while the investigation is pending.

4.6 Traceback response and cooperation commitment

The Company commits to respond within 24 hours to all traceback requests from the Federal Communications Commission, civil or criminal law enforcement, and the registered industry traceback consortium. The Company also commits to cooperate with such entities in investigating and stopping illegal robocallers that use the Company's service to originate, carry, or process calls.

- Primary traceback contact: Keven Vrotney, COO, keven@kainnovations.com, 423-670-6008.
- Backup traceback contact: Ashley Baldwin, CEO, ashley@kainnovations.com, 423-430-6799.
- Traceback intake channel(s): support@kainnovations.com, internal management escalation, and direct phone response procedures.
- The Company preserves and can retrieve relevant call detail records, provisioning records, customer records, and related account information needed to investigate traceback requests.
- If a traceback identifies apparently illegal or suspicious calling, the Company will promptly investigate and take appropriate mitigation measures, which may include blocking, suspension, termination, number removal, or referral to upstream providers or law enforcement as appropriate.

4.7 Enforcement actions and remediation

When the Company determines that a customer, reseller, or traffic source is engaged in illegal robocalling, spoofing, or materially deceptive conduct, the Company may take one or more of the following actions based on the facts and severity of the matter:

- Require additional information or proof of consent, identity, number authorization, or calling purpose.
- Impose outbound restrictions, caller-ID restrictions, rate limits, destination limits, or account holds.
- Block traffic, deactivate numbers, suspend service, or terminate the relationship for violation of law or Company policy.
- Notify underlying providers, downstream partners, and appropriate investigative authorities when warranted.
- Document the event and retain records of the investigative steps and remedial measures taken.

4.8 Governance, training, and record retention

The Company assigns responsibility for robocall mitigation to Executive management and operations leadership. Relevant personnel are trained on onboarding controls, traceback obligations, complaint handling, and escalation rules. The Company retains the records reasonably necessary to support this plan, the Company's RMD filing, customer onboarding decisions, and traceback responses for at least at least two years or longer if required by law, contract, or an active investigation.

- Periodic review of this plan: At least annually and sooner after material operational, ownership, regulatory, or provider-platform changes..
- Responsible owner of plan updates: Keven Vrotney, COO.
- Internal departments involved: Operations, executive management, customer service, and any external advisors engaged for compliance support.

5. Optional supplemental responses for the RMD form

The FCC permits filers to place overflow information from certain RMD text boxes in the mitigation plan, so long as the filing identifies the applicable section. Use this section only if additional space is needed.

Potential form item	Supplemental response
Principals	Ashley Baldwin - CEO; Keven Vrotney - COO.
Affiliates / subsidiaries / parent companies	None.
Prior formal actions or investigations in last two years	None.
Foreign voice service provider explanation	Not applicable. K & A Innovations, LLC is not a foreign voice service provider.
Any additional explanatory text for the filing	Section 5 may be used to support the filing responses for the voice service provider, gateway provider, and non-gateway intermediate provider explanations if any RMD text box is too short.

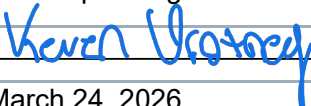
Voice service provider explanation for Option 3: K & A Innovations, LLC is a white-label voice service provider/reseller that uses SkySwitch as its underlying platform and does not independently control the network infrastructure necessary to implement STIR/SHAKEN for the voice service provider function. K & A Innovations, LLC relies on the underlying upstream platform/provider for network-level STIR/SHAKEN implementation where applicable. K & A Innovations, LLC nevertheless subjects all calls it originates on its network to its robocall mitigation program, including customer vetting, traffic monitoring, traceback cooperation, and response within 24 hours.

Gateway provider explanation for Option 3: To the extent this filing requires a gateway-provider certification, K & A Innovations, LLC is unable to implement STIR/SHAKEN for any gateway-provider function because it lacks control over the network infrastructure necessary to do so. K & A Innovations, LLC does not independently operate gateway-provider network facilities for directly receiving traffic from foreign providers at U.S.-based facilities and instead relies on its underlying provider/platform where applicable. K & A Innovations, LLC nevertheless maintains a robocall mitigation program and responds to traceback requests within 24 hours.

Non-gateway intermediate provider explanation for Option 3: To the extent this filing requires a non-gateway intermediate-provider certification, K & A Innovations, LLC is unable to implement STIR/SHAKEN for that function because it lacks control over the network infrastructure necessary to do so. K & A Innovations, LLC does not independently operate non-gateway intermediate-provider signaling/authentication infrastructure and instead relies on its underlying provider/platform where applicable. K & A Innovations, LLC nevertheless maintains a robocall mitigation program, investigates suspicious activity, cooperates with traceback efforts, and responds to traceback requests within 24 hours.

6. Officer approval

This plan has been reviewed and approved by an officer of the Company authorized to oversee robocall mitigation compliance and the Company's RMD filing.

Name	Keven Vrotney
Title	Chief Operating Officer
Signature	
Date	March 24, 2026

Appendix A. Quick cross-reference for the RMD portal

Portal topic	Where to point in this plan
STIR/SHAKEN status explanation	Section 3
Know-your-customer procedures	Section 4.1
Upstream provider procedures	Section 4.2
Analytics vendor or statement that no analytics are used	Section 4.4
24-hour traceback commitment and cooperation statement	Section 4.6
Supplemental long-form answers	Section 5