

ROBOCALL MITIGATION PLAN

Grigoryans Technology Keystone dba KeystoneTelX

Legal Entity Name	GRIGORYANS TECHNOLOGY KEYSTONE
DBA / Brand	KeystoneTelX
Underlying Platform	SkySwitch (Wholesale VoIP Provider)
FCC Filing Tier	47 CFR §64.6305(d)(1)(iii) — No STIR/SHAKEN Implementation
Plan Effective Date	April 15, 2026
Plan Version	2.0
Responsible Officer	Tigran Grigoryan, CEO
Compliance Email	support@keystonetelx.com
Compliance Phone	888-797-9188

Submitted in compliance with 47 CFR Part 64, Subpart Z and filed with the FCC Robocall Mitigation Database.

1. Purpose and Scope

This Robocall Mitigation Plan ("Plan") documents the policies, procedures, and controls implemented by Grigoryans Technology Keystone dba KeystoneTelX ("KeystoneTelX") to prevent the origination and transmission of illegal robocall traffic. This Plan is prepared pursuant to FCC rules implementing the TRACED Act (Pallone-Thune TELEPHONE Robocall Abuse Criminal Enforcement and Deterrence Act), codified at 47 CFR Part 64, Subpart Z.

KeystoneTelX operates as a reseller of VoIP telecommunications services utilizing the SkySwitch wholesale platform. KeystoneTelX does not own or operate its own switching infrastructure and does not independently sign calls using STIR/SHAKEN credentials. KeystoneTelX files under 47 CFR §64.6305(d)(1)(iii) — certifying that it has not implemented STIR/SHAKEN on any portion of its network — and relies on SkySwitch for network-level call authentication, focusing its mitigation obligations at the customer-facing layer by filing an annual certification with the FCC Robocall Mitigation Database.

KeystoneTelX has not been prohibited from filing a certification in the Robocall Mitigation Database.

KeystoneTelX does not have a history of enforcement actions for illegal robocalls, TCPA or TSR violations, or related state law violations.

This Plan applies to all VoIP services resold under the KeystoneTelX brand and to all customer accounts provisioned through the KeystoneTelX reseller portal.

3. Upstream Provider — SkySwitch

KeystoneTelX's voice services are delivered exclusively through SkySwitch, a licensed wholesale VoIP provider. KeystoneTelX has confirmed that SkySwitch:

- Implements STIR/SHAKEN on all IP-originated calls traversing its network;
- Holds a valid SPC token and is listed in the FCC Robocall Mitigation Database as a compliant provider;
- Maintains its own robocall mitigation policies and is contractually bound to comply with applicable FCC rules;
- Provides flow-down contractual obligations requiring KeystoneTelX, as reseller, to prohibit illegal robocalling by customers and to comply with applicable law.

KeystoneTelX does not alter, strip, or manipulate STIR/SHAKEN identity headers on calls passing through its reseller layer. KeystoneTelX will notify SkySwitch promptly upon learning of any customer activity that may compromise the integrity of call authentication on the platform.

KeystoneTelX will periodically verify that SkySwitch remains in good standing on the FCC Robocall Mitigation Database and will update this Plan if the upstream provider relationship changes.

4. Customer Onboarding and Know Your Customer (KYC)

4.1 Standard Onboarding Verification

Prior to activating service, KeystoneTelX requires all new customers to complete the following steps:

- Provide the legal name of the business entity or individual account holder;
- Submit a valid government-issued business registration document (EIN confirmation, state business license, or Articles of Incorporation) or, for individuals, a government-issued photo ID;
- Confirm a physical service address (P.O. boxes are not accepted as the sole address of record);
- Provide a working contact phone number and primary email address;
- Execute KeystoneTelX's Acceptable Use Policy (AUP) and Service Agreement, which expressly prohibit illegal robocalling;
- Disclose the intended use case for any outbound calling volume exceeding normal business thresholds.

4.2 High-Risk Account Enhanced Review

The following characteristics trigger enhanced review prior to service activation:

- Requests for an unusually large quantity of DIDs at initial signup;
- Stated use cases involving high-volume outbound campaigns (telemarketing, political dialing, debt collection, or similar);
- Prepaid or cash-equivalent payment without verifiable business history;
- Geographic inconsistency between stated business location, billing address, and IP of origin;
- Prior service terminations for cause with KeystoneTelX or any upstream or affiliated provider.

Enhanced review measures may include direct phone or video verification with the account holder, review of prior carrier references, and execution of a supplemental acknowledgment specifically prohibiting robocall traffic.

5. Acceptable Use Policy (AUP) Enforcement

KeystoneTelX's Acceptable Use Policy expressly prohibits customers from using KeystoneTelX services to:

- Originate calls that violate the Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227;
- Transmit calls with spoofed or falsified caller ID information in violation of the Truth in Caller ID Act;

- Conduct autodialed or prerecorded message campaigns without required prior express written consent;
- Call numbers listed on the National Do Not Call Registry without a valid exemption;
- Engage in call flooding, SIP-based denial of service, or any abuse of the PSTN;
- Resell, sublease, or share KeystoneTelX services with third parties for calling purposes without prior written approval.

Violation of the AUP is grounds for immediate service suspension without advance notice.

KeystoneTelX may block the originating number(s), terminating numbers(s), trunk(s) or customer, including termination of customer relationship to prevent robocalling, invalid originating number or spoofed origination number.

KeystoneTelX reserves the right to terminate service permanently for repeat or willful violations and to report violating customers to the FCC, the FTC, and applicable law enforcement authorities.

6. Traffic Monitoring and Anomaly Detection

6.1 Baseline Traffic Profiling

Upon account activation, KeystoneTelX establishes a baseline call volume expectation based on the customer's stated use case. Significant deviations from this baseline trigger manual account review. Indicators monitored include:

- Sudden spikes in outbound call volume;
- High ratios of short-duration calls (indicative of robocall campaigns);
- Unusually high call failure rates or ring-no-answer patterns;
- Calls originating to sequential or numerically adjacent telephone numbers;
- Repeated calls to numbers identified on Do Not Call or known litigant lists.

6.2 Complaint Monitoring

KeystoneTelX monitors the following channels for complaints related to illegal calling activity:

- FCC consumer complaints referencing KeystoneTelX-originated or KeystoneTelX-transited calls;
- Direct complaints received via KeystoneTelX support channels;
- Notices from SkySwitch or other upstream carriers regarding suspicious traffic;
- Traceback requests from the Industry Traceback Group (ITG).

All complaints are logged with date, nature of complaint, and customer account involved. KeystoneTelX will investigate and resolve complaints within five (5) business days and document the outcome.

7. Traceback Response Procedures

KeystoneTelX will respond fully and promptly to traceback requests from the Industry Traceback Group (ITG) and the FCC, in accordance with 47 CFR §64.6308. KeystoneTelX's traceback response procedure is as follows:

- Upon receipt of a traceback inquiry, KeystoneTelX will acknowledge receipt within 24 hours;
- KeystoneTelX will identify the customer account associated with the subject call using call detail records (CDRs) available through the SkySwitch platform;
- KeystoneTelX will provide requested information (customer identity, call records, and account details) to the ITG or FCC;
- Where a customer is identified as the source of illegal robocall traffic, KeystoneTelX will suspend the account pending investigation and notify SkySwitch;
- KeystoneTelX will cooperate with any subsequent FCC enforcement inquiry or law enforcement investigation.

9. Staff Training and Awareness

KeystoneTelX ensures that personnel involved in customer onboarding, account management, and technical support are trained on:

- FCC robocall rules and KeystoneTelX's obligations as a voice service provider filing under 47 CFR §64.6305(d)(1)(iii);
- Identification of high-risk account characteristics and internal escalation procedures;
- The requirements and procedures set forth in this Plan;
- How to receive, log, and route traceback requests and FCC/ITG inquiries to the responsible officer.

Training is conducted at onboarding for new staff and reviewed annually, or whenever material changes to FCC rules or this Plan occur.

10. Plan Review and Maintenance

KeystoneTelX will review and update this Plan:

- Annually, at minimum, in conjunction with FCC Robocall Mitigation Database certification renewal;
- Upon any material change to KeystoneTelX's service offerings, upstream provider relationship, or customer base;
- Upon issuance of new FCC rules, orders, or guidance affecting providers certifying under 47 CFR §64.6305(d)(1)(iii);
- Following any significant robocall incident, traceback action, or FCC enforcement inquiry involving KeystoneTelX.

The responsible officer identified on the cover page is accountable for maintaining this Plan and ensuring timely annual FCC database certification.

11. Certification

I, Tigran Grigoryan, on behalf of Grigoryans Technology Keystone dba KeystoneTelX, certify under penalty of perjury that:

- The information contained in this Robocall Mitigation Plan is accurate and complete to the best of my knowledge;
- KeystoneTelX has implemented, or will implement, the robocall mitigation measures described herein;
- KeystoneTelX will not knowingly originate illegal robocall traffic and will take prompt action to investigate and stop any such traffic identified on its network;
- KeystoneTelX will respond to traceback requests from the ITG and the FCC in the time and manner required by applicable law;
- KeystoneTelX will update this Plan and its FCC Robocall Mitigation Database certification as required by FCC rules.



Signature

04/15/2026

Date

TIGRAN GRIGORYAN

Printed Name

CEO

Title

April 15, 2026