

ROBOCALL MITIGATION PROGRAM (ORIGINATING VOICE SERVICE PROVIDER – WHITE-LABEL SKYSWITCH)

Provider Role: Originating Voice Service Provider (VSP)

Business Model / Network Context: We provide interconnected VoIP voice service to end customers and resellers under our brand and **white-label the SkySwitch platform** for call control and service delivery. We are responsible for (a) onboarding and monitoring our originating customers/resellers, (b) enforcing acceptable use and anti-abuse controls, and (c) coordinating technical mitigation actions with our underlying platform/provider partners as needed.

1) 24-Hour Traceback Commitment and Cooperation

We respond to traceback requests from the FCC, law enforcement, and the industry traceback consortium **within 24 hours** of receipt. We maintain a dedicated escalation path for traceback requests and will promptly provide relevant call records and routing/customer information, cooperate with investigations, and take action to stop illegal robocall origination on our service.

Operational handling: Traceback requests are treated as high-priority incidents; we acknowledge receipt promptly, produce requested records (e.g., CDRs, SIP signaling details where available, account/trunk identifiers), identify the originating customer/reseller, and implement appropriate mitigation actions (blocking/suspension/termination) as warranted.

2) Know-Your-Customer (KYC) and Customer Due Diligence (Originating)

We take reasonable steps to know our originating customers (including resellers) before enabling outbound origination and throughout the customer lifecycle. Our onboarding and due diligence include:

- **Identity verification:** Legal entity name, address, responsible individual(s), and verification of business registration/Tax ID (or equivalent evidence).
- **Service/use-case validation:** Declared calling use-case(s), expected volumes, and campaign types (if applicable).
- **Numbering authorization:** Confirmation of the customer's right to use numbers presented as caller ID (e.g., assignment/porting documentation, LOA where applicable, inventory records, or other evidence).
- **Risk screening:** Enhanced review for higher-risk profiles (e.g., lead generation, unusually high anticipated volumes, short-duration trial requests, opaque ownership, prior compliance signals).

- **Contractual controls:** Customer/reseller agreements include prohibitions against illegal robocalls/spoofing, requirements to comply with applicable laws, requirements to cooperate with investigations/tracebacks, and provisions allowing us to suspend or terminate service for suspected abuse.

We perform **ongoing KYC refresh** when triggered by abnormal traffic patterns, complaint spikes, traceback involvement, changes in ownership/control, or other risk indicators.

3) Traffic Monitoring, Analytics, and Detection

We use traffic monitoring and analytics to identify and mitigate likely illegal robocall and spoofing activity originating on our service. Detection methods may include:

- **Anomaly monitoring:** Sudden spikes in call volume, burst patterns, irregular time-of-day behavior, and atypical geographic/call distribution patterns.
- **High-failure / short-duration patterns:** Elevated ASR anomalies, very short average call duration, repeated attempts to many destinations, and sequential/automated dialing characteristics.
- **Invalid/abusive calling indicators:** Invalid caller ID formats, unallocated/invalid numbering patterns, high complaint/reputation signals, and other indicators of spoofing or abusive behavior.
- **Customer/reseller-level scoring:** Monitoring at trunk/account/campaign level to identify sources generating disproportionate negative signals.

Analytics tooling: We use a combination of platform capabilities (including SkySwitch-provided reporting/controls) and our internal monitoring and review processes. Where third-party analytics are used, we maintain an up-to-date record of the vendor(s) and operational use.

4) Mitigation Actions (Blocking / Suspension / Termination)

When traffic is flagged as suspected illegal robocall activity, spoofing, or a violation of our acceptable use requirements, we take proportionate mitigation actions, which may include:

- **Rate limiting / throttling** at the account/trunk level
- **Targeted blocking** of specific sources (accounts, trunks, destinations, or calling patterns)
- **Immediate suspension** of outbound calling privileges pending investigation
- **Remediation requirements** (KYC refresh, proof of consent/compliance documentation, use-case restrictions, dialing behavior changes)
- **Termination** for repeated violations or severe/egregious abuse

All mitigation actions are documented with timestamps, reason codes, affected identifiers (customer/reseller/account/trunk), approving personnel, and final disposition.

5) STIR/SHAKEN Call Authentication (Status and Controls)

We maintain accurate certifications regarding our STIR/SHAKEN implementation status and practices. Where we sign calls, we apply appropriate attestation based on our knowledge of the customer and their authorization to use calling numbers, and we maintain controls to prevent inappropriate attestation.

Implementation note: Because we deliver service via a white-labeled platform, our STIR/SHAKEN signing/verification capability may be implemented through the SkySwitch ecosystem and/or associated interconnection partners. We coordinate configuration, monitoring, and remediation with the underlying platform/provider partners to ensure our certified status remains accurate.

6) Complaint Intake, Investigation, and Enforcement

We maintain an abuse/complaint intake channel and operational process to investigate suspected illegal robocall activity, including:

- Centralized intake (robocallabuse@netstandard.com/generates a ticket ITSM)
- Triage and investigation workflow that correlates complaints to accounts/trunks/traffic patterns
- Escalation to mitigation actions (Section 4) when warranted
- Evidence preservation and case documentation for traceback/enforcement support

7) Recordkeeping and Retention

We retain records sufficient to support traceback and enforcement cooperation, including:

- Customer/reseller onboarding artifacts and KYC documentation
- Call detail records and supporting signaling/routing data reasonably available
- Logs of analytics findings, investigations, and mitigation actions taken
- Copies of RMD submissions and material change/update history

Records are retained for a minimum period consistent with our compliance needs and contractual/legal requirements.

8) Program Governance and Updates

This program is owned by our Compliance/Regulatory function with operational support from our Network/Voice Operations team. We review robocall mitigation performance and controls at least quarterly and update internal procedures as needed. We maintain accurate RMD information and update the RMD filing promptly when required information changes (e.g., contact information, mitigation approach, platform/provider relationships that materially affect our mitigation program).