

Contents

Principals, Affiliates, Subsidiaries, and Parent Companies:.....	1
Program Overview.....	2
Regulatory Compliance Statement	2
Program Components	2
Network Monitoring and Traffic Analysis	2
□ Investigate traffic spikes or patterns consistent with auto-dialer activity.....	2
Program Components (continued).....	2
Auto-monitoring platform generated reports.....	3
Caller Identification and Vetting	3
Conduct Know Your Customer (KYC) procedures for all new and existing customers. Require valid identification and business purpose for customers seeking high-volume outbound calling services. Some of the requirements are as follows:.....	3
Verify the legitimacy of customer-provided numbers through industry databases (e.g., CNAM, LRN).....	3
Call Authentication.....	4
Blocking and Labeling Mechanisms	4
Complaint Intake and Investigation.....	5
Cooperation with Industry and Law Enforcement.....	5
Recordkeeping and Reporting	5
Employee Training	5
Program Review and Continuous Improvement.....	5
Documentation and Certification.....	5
Contact Information.....	6

Principals, Affiliates, Subsidiaries, and Parent Companies:

- Principal: David W Clark, Managing Member
- Affiliates: Aaron Archambault, Managing Member
- Subsidiaries: IPnetvoice LLC FRN #0031421696, CommSyncIT LLC FRN #0037445350-
Parent Company: Sky Link LLC

Program Overview

This Robocall Mitigation Program (“Program”) is designed to prevent the origination, transmission, and/or termination of illegal robocalls on Sky Link LLC’s network. The Program implements reasonable practices to identify and block unlawful robocall traffic, in accordance with 47 CFR § 64.6305(a) and the FCC’s Robocall Mitigation Database (RMD) requirements.

Regulatory Compliance Statement

Sky Link LLC certifies that it has implemented a robocall mitigation program consistent with the requirements of 47 CFR § 64.6305(a) and has filed the required certification and program description with the FCC Robocall Mitigation Database.

Program Components

Network Monitoring and Traffic Analysis

Regularly monitor call traffic patterns for anomalies indicative of illegal robocalling (e.g., high call volumes, short call durations, sequential dialing). Use analytics tools and reporting systems to flag suspicious calling behavior.

- Investigate traffic spikes or patterns consistent with auto-dialer activity.
 - Auto-monitoring by managing platform report tools to FLAG:
 - All DID numbers for an account that transmit to a same number more than four (4) times in a 10 second period
 - Maintain and validate email and physical addresses in the Platforms database.
 - Customer accounts have limited minute plans & limited amount of DID numbers per customer account not to exceed 20
 - SMS transmissions are not authorized unless a “plan of use & action” is filed and approved by the platform compliance officer and or CommSyncIT LLC its affiliates & subsidiaries.
 - Customer Accounts that exceed the limited minute plans and is in excess of 100% of its limited minute plan allocation

Program Components (continued)

Auto-monitoring platform generated reports

Daily, Weekly, Monthly report generation:

- All customer accounts must have inbound activity to 80% of all DID numbers.
- All customer accounts must have an Owner of the Account and provide contact information as such with email address, physical address, and mailing address, on file.
- Flag customer accounts
- This will generate an email to the owner of the account to explain the variance identified with Robocalling. A 15 day grace period for the customer to reply to the following:
- Repetitive outbound transmissions to the same number not longer than four (4) seconds within a 20-second window of time per DID number on account.
- Repetitive outbound transmissions to the same number not longer than four (4) seconds using more than one DID number associated with the account.
- Restrict customer accounts
- Non-compliance of any of the above without an explanation from the Owner of Account will be inoperable for outbound transmissions until all communications satisfy the Platform Compliance Department, CommSyncIT LLC, its affiliates & subsidiaries.

Caller Identification and Vetting

Conduct Know Your Customer (KYC) procedures for all new and existing customers. Require valid identification and business purpose for customers seeking high-volume outbound calling services. Some of the requirements are as follows:

- TIN #
- Foreign or Domestic State filing status
- Multiple State Activity
- Owner of Account (physical address, email address, website SSL & DNS certifications)

Verify the legitimacy of customer-provided numbers through industry databases (e.g., CNAM, LRN).

CNAM (Caller Name) Lookup

- Confirms whether the caller ID name matches the expected entity.
- Helps detect mismatches between claimed identity and registered CNAM data.
- Supports trust and reduces spoofing risk

LRN (Local Routing Number) Lookup

- Confirms the carrier of record for a number.
- Helps detect numbers that are unassigned, disconnected, or ported unexpectedly.
- Useful for validating that a customer actually controls the number they claim

Program Components (continued)

Industry Number Databases

- NPAC (Number Portability Administration Center): Confirms number ownership and porting history.
- Line Type Databases: Identifies whether a number is wireless, VoIP, landline, or toll free.

KYC (Know Your Customer) Identity Verification

- Collecting business documentation (EIN, articles of incorporation, utility bills).
- Verifying the customer's legal identity and authority to use the numbers they provide.
- Often paired with fraud risk scoring.

Traffic Pattern Analysis

Monitoring for high risk behaviors such as:

- Short-duration calls
- High-volume bursts
- Sequential dialing

Reputation and Analytics Databases

- Using third-party analytics (e.g., spam score providers) to detect suspicious numbers.
- Helps prevent numbers already flagged as spam from being used.

Proof-of-Control Checks

- Sending a verification code to the number.
- Requiring customers to respond from the number they claim to own.

Foreign or Domestic State filing status

- Multiple State Activity
- Owner of Account (physical address, email address, website SSL & DNS certifications)
- Number of DID numbers limited to the amount of twenty (20)
- Conduct a search of DID numbers being considered to transfer
- Conduct a search Better Business Bureau of the customer considering to transfer

Call Authentication

- Implement STIR/SHAKEN call authentication technology for IP-based traffic as required.
- For non-IP traffic, employ best available practices to authenticate caller identity, such as call traceback and manual verification.

Blocking and Labeling Mechanisms

Block calls from numbers known to be associated with illegal robocalling, as identified by industry traceback consortia or regulatory authorities.

Label suspected robocalls to end-users when blocking is not feasible.

Complaint Intake and Investigation

Maintain a dedicated contact channel (email/phone) for robocall complaints from subscribers, carriers, and the public.

Investigate complaints promptly and take remedial action when warranted (e.g., warn, suspend, or terminate offending customers).

Cooperation with Industry and Law Enforcement

Participate in industry traceback initiatives (e.g., USTelecom Industry Traceback Group).

Cooperate with law enforcement and regulatory bodies in investigations of illegal robocall campaigns.

Recordkeeping and Reporting

Retain records of mitigation efforts, customer vetting, traffic analysis, and complaint resolutions for at least 12 months.

File annual certifications and program updates with the FCC Robocall Mitigation Database as required.

Employee Training

Provide regular training to employees on robocall mitigation procedures, regulatory requirements, and customer vetting.

Program Review and Continuous Improvement

Conduct quarterly reviews of the Program's effectiveness.

Update mitigation practices in response to evolving threats and regulatory changes.

Documentation and Certification

Maintain detailed documentation of all mitigation activities, procedures, and outcomes.

Ensure timely submission of the Robocall Mitigation Certification and Program Description to the FCC RMD.

Contact Information

Robocall Mitigation Point of Contact:

David W. Clark
Founder & SVP of
Operations
HQ in Vermont
Help Desk: (802) 9922100
ext 102
Cell Phone: (518) 572-
6118

This program template serves as a robust and compliant approach to robocall mitigation for service providers. Customize with your company's specific details and operational practices as needed to ensure accuracy and compliance.