

ROBOCALL MITIGATION PLAN

Filed pursuant to 47 C.F.R. § 64.6305(b) and (c)

SECTION 1 — FILER IDENTIFICATION

Field	Value
Legal Entity Name	[EXACT name on Articles of Organization – e.g. SipCommander LLC]
Doing Business As	[DBA if any, otherwise "N/A"]
FCC Registration Number (FRN)	[From CORES]
FCC Form 499 Filer ID	[From USAC – required before RMD submission]
Operating Company Number (OCN)	[If none, enter "None – non-facilities-based reseller"]
Business Address	[Street address you control]
Business Phone	[Main business line]
Email	[Working email – monitored]
Date of Filing	[Date]

Provider Classification

[SELECT ONE – delete the others]

- ☒ Facilities-based voice service provider
- ☒ **Non-facilities-based voice service provider (reseller)**
- ☐ Intermediate provider
- ☐ Gateway provider

Note: If you are reselling SIP trunks over an upstream carrier's network and do not own switching/transport facilities, you are a **non-facilities-based provider (reseller)**. Do not check "Gateway provider" unless you accept traffic entering the US from outside it — gateway providers carry substantially heavier obligations under 47 C.F.R. § 64.1200(n).

Contact for Traceback and Law Enforcement Requests

Field	Value
Name	[Named individual – not a generic alias]
Title	[e.g. Managing Member]
Phone	[Answered during US business hours]
Email	[Monitored daily]

This contact must be reachable. The Industry Traceback Group (ITG) will use it, and non-response to traceback requests is itself an enforcement trigger.

SECTION 2 — STIR/SHAKEN IMPLEMENTATION STATUS

[SELECT ONE – delete the others]

- **(a) Complete STIR/SHAKEN implementation.** All SIP calls originated are authenticated and signed with the filer's own STI certificate.
- **(b) Partial STIR/SHAKEN implementation.** Some portion of traffic is signed; the remainder is covered by the mitigation program in Section 3.
- **(c) No STIR/SHAKEN implementation.** The filer has not obtained an STI certificate and relies entirely on the robocall mitigation program in Section 3.

Statement of Current Status

[WRITE THE TRUTH. Template for a reseller whose upstream signs:]

The filer is a non-facilities-based reseller of SIP trunking services and does not currently hold its own Service Provider Code (SPC) token or STI certificate. The filer does not operate its own softswitch or session border controller capable of applying SHAKEN attestation. All voice traffic originated by the filer's customers is transmitted to and terminated by [UPSTREAM CARRIER LEGAL NAME], which holds OCN [OCN] and is listed in the Robocall Mitigation Database. [UPSTREAM] applies STIR/SHAKEN authentication and attestation to the filer's traffic prior to handoff to downstream networks, pursuant to the service agreement dated [DATE]. The filer is pursuing its own OCN and SPC token, with an anticipated completion of [REALISTIC TARGET – or delete this sentence if you have no such plan].

■ **Verify before filing:** Confirm in writing with your upstream that they sign your traffic and at what attestation level (A, B, or C). Do not assert this if you have not confirmed it. Many wholesale carriers sign at **B or C** attestation for reseller traffic, not A — and some do not sign reseller traffic at all.

SECTION 3 — ROBOCALL MITIGATION PROGRAM

Required under 47 C.F.R. § 64.6305(c) for any provider not fully implementing STIR/SHAKEN. The program must include "reasonable steps to avoid originating illegal robocall traffic" and a commitment to "respond fully and in a timely manner to all traceback requests."

3.1 Know Your Customer (KYC) — Onboarding Due Diligence

Before provisioning service to any customer, the filer collects and verifies:

1. **Legal entity verification** — Legal business name, state of formation, entity registration number, and EIN. Verified against the applicable Secretary of State public registry.
2. **Beneficial ownership** — Identity of each person owning 25% or more, including government-issued photo identification.
3. **Authorized representative** — Name, title, direct phone, and email of the individual executing the service agreement.
4. **Physical business address** — Verified as a genuine premises; virtual-office and mail-drop addresses are flagged for enhanced review.
5. **Use case statement** — A written description of intended calling: purpose, expected call volume, average call duration, geographic distribution, and whether the traffic is inbound, outbound, or both.
6. **Consent basis** — For any outbound campaign traffic, written documentation of the legal basis for calling, including prior express consent where required under the TCPA.
7. **Number ownership** — Evidence of the customer's right to use any telephone numbers presented as caller ID, whether owned, ported, or delegated.
8. **Prior provider history** — Disclosure of previous voice providers and the reason for any prior termination or suspension.

Prohibited customers. The filer will not knowingly provision service to any person or entity that: is subject to an FCC cease-and-desist or enforcement action; has been removed from the Robocall Mitigation Database; appears on an ITG non-responsive provider list; refuses to provide the documentation above; or declines to identify beneficial ownership.

3.2 Acceptable Use Policy and Contractual Terms

Every customer agreement incorporates binding terms that:

- Prohibit origination of illegal robocalls, including any call violating the TCPA, the Truth in Caller ID Act, or FCC rules;
- Prohibit unlawful caller ID spoofing and require that any caller ID presented be a number the customer is authorized to use;
- Require the customer to maintain and produce, within 24 hours of request, consent records and campaign documentation for any traffic subject to traceback;
- Grant the filer the right to suspend or terminate service **immediately and without notice** upon credible evidence of illegal traffic;
- Prohibit resale or sub-delegation of service without the filer's prior written consent, and

require any approved sub-reseller to adopt equivalent KYC and AUP obligations;

- Require the customer to cooperate fully with any traceback or law enforcement inquiry.

3.3 Ongoing Traffic Monitoring

The filer monitors traffic for indicators of illegal calling, including:

Indicator	Threshold / Action
Average call duration below 10 seconds	Flag for review
Answer-seizure ratio (ASR) below [X]%	Flag for review
Sudden volume increase above [X]× baseline	Flag for review
High call volume to a single NPA-NXX	Flag for review
Calls to numbers on the Do Not Originate (DNO) list	Block
Invalid, unallocated, or unassigned calling numbers	Block
Caller ID not provisioned to the customer	Block
Elevated intercept/SIT response rates	Flag for review
Complaints received from downstream carriers	Immediate investigation

[FILL IN REAL THRESHOLDS – or if your upstream provides the monitoring, state that plainly and name the tooling. Do not describe monitoring you do not perform.]

Review cadence. Traffic analytics are reviewed [daily / weekly – state the truth]. Flagged accounts are investigated within [X] business hours.

3.4 Escalation and Enforcement

Upon detection of suspected illegal traffic:

1. **Hour 0–4** — Account flagged; the filer notifies the customer in writing and requests documentation substantiating the traffic's legality.
2. **Hour 4–24** — If documentation is not provided or is inadequate, outbound calling is **suspended**.
3. **Within 48 hours** — If illegality is confirmed, the account is **terminated**, the filer's upstream provider is notified, and the matter is documented.
4. **Repeat or egregious conduct** — Immediate termination without the graduated steps above.

All actions are logged with timestamp, the evidence relied upon, the decision maker, and the outcome. Logs are retained for not less than **two years**.

3.5 Traceback Response

The filer commits to respond **fully and in a timely manner** to all traceback requests from the Commission, from civil or criminal law enforcement, and from the industry traceback consortium (USTelecom's Industry Traceback Group).

- **Response target:** within **24 hours** of receipt, and in all cases within the deadline stated in the request.
- The filer maintains call detail records sufficient to identify the immediate upstream source and the originating customer for every call it transmits.
- CDRs are retained for not less than **two years**.
- The traceback contact in Section 1 is monitored on business days and is authorized to act.

3.6 Records Retention

Record Type	Retention
Customer KYC documentation	Term of service + 2 years
Signed customer agreements	Term of service + 2 years
Call detail records	2 years minimum
Traceback requests and responses	2 years minimum
Traffic monitoring alerts and dispositions	2 years minimum
Suspension and termination records	2 years minimum

3.7 Governance and Review

This plan is reviewed not less than **annually**, and additionally upon any material change to the filer's network, upstream providers, customer base, or applicable FCC rules. The individual named in Section 1 is responsible for implementation and for maintaining the accuracy of this filing.

The filer will update its Robocall Mitigation Database entry within **10 business days** of any change rendering this filing inaccurate, as required by 47 C.F.R. § 64.6305(b)(4).

SECTION 4 — CERTIFICATION

■ **This is sworn under penalty of perjury. Read it before signing.**

I, [FULL LEGAL NAME], [TITLE] of [LEGAL ENTITY NAME], hereby certify under penalty of perjury that:

1. I am an officer or authorized representative of the filer with authority to make this certification;
2. I have personal knowledge of the filer's robocall mitigation practices described herein;

3. The information in this filing is true, complete, and accurate to the best of my knowledge, information, and belief;
4. The filer has implemented the robocall mitigation program described in Section 3, and that program is **currently operational** — not merely planned;
5. The filer commits to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium;
6. The filer will update this filing within 10 business days of any material change.

Signature	_____
Printed Name	[FULL LEGAL NAME]
Title	[TITLE]
Date	[DATE]

APPENDIX A — PRE-FILING CHECKLIST

Do not submit until every box is checked.

- ☒ LLC formed; Articles of Organization filed and approved
- ☒ EIN obtained from the IRS
- ☒ FRN obtained via FCC CORES (Form 160) — entity type **Private Sector**
- ☒ FCC Form 499-A filed; **Filer ID received** (*RMD submission requires it*)
- ☒ Upstream carrier agreement executed
- ☒ **Written confirmation from upstream** that they apply STIR/SHAKEN to your traffic, and at what attestation level
- ☒ Section 2 status selected and accurate
- ☒ Every [bracketed placeholder] replaced with a real value
- ☒ Every monitoring threshold in 3.3 filled with a number you actually enforce
- ☒ KYC process in 3.1 actually built — intake form, ID collection, verification step
- ☒ Customer agreement drafted with the AUP terms in 3.2
- ☒ Traceback contact live and monitored
- ☒ CDR retention configured for 2 years
- ☒ Reviewed by telecom counsel

File at: <https://fccprod.servicenowservices.com/rmd>

APPENDIX B — WHY ACCURACY MATTERS HERE

The Robocall Mitigation Database is not a formality. Specific exposure:

- **Removal from the RMD** bars every US voice provider from accepting your traffic (47 C.F.R. § 64.6305(g)). This is an existential outcome for a reseller, and the FCC has removed thousands of filings for deficiency.
- **Forfeiture penalties** have been issued for certifications that did not match actual operations.
- **False certification** is sworn under penalty of perjury — 18 U.S.C. § 1001 exposure, separate from FCC penalties.
- **Gateway provider misclassification** carries heavier obligations under 47 C.F.R. § 64.1200(n). Classify honestly.

A plan describing a KYC process you have not built, monitoring you do not perform, or an upstream signing arrangement you have not confirmed is a **deficient filing** even if everything else is in order. Build the program first, then certify it.

Prepared as a working template. Not legal advice. Have telecom counsel review before filing — this is the single highest-exposure document in your regulatory stack.