
Robocall Mitigation Plan

Mobile Access Consumer Services LLC (MACS)
Robocall Mitigation Plan
Filed Pursuant to 47 CFR § 64.6305

1. Provider Identification

Legal Entity: Mobile Access Consumer Services LLC
Business Type: VoIP Reseller / UCaaS Provider
Address: Franklinville, NJ
FCC Registration Number (FRN): 0038392767
RMD Filing Category: Voice Service Provider without a STIR/SHAKEN obligation

Justification:

MACS does not control the network elements required to authenticate caller ID. All SIP origination, PSTN interconnection, numbering resources, and STIR/SHAKEN signing are performed by MACS's upstream provider, SkySwitch and its underlying carriers.

2. STIR/SHAKEN Status

MACS does **not** have a STIR/SHAKEN implementation obligation under:

- **47 CFR § 64.6301(a)** (applies only to providers that originate SIP calls into the PSTN)
- **47 CFR § 64.6303** (exemption for providers lacking control of authentication infrastructure)

MACS relies on its upstream provider's fully deployed STIR/SHAKEN implementation. MACS does not possess or operate:

- SIP authentication services
- STI-CA certificates
- STI-AS or STI-VS functions
- Numbering resources
- PSTN interconnection facilities

MACS therefore files as a **Voice Service Provider without a STIR/SHAKEN obligation**.

3. Overview of MACS's Robocall Mitigation Program

MACS maintains a **multi-layered robocall mitigation program** designed to prevent the origination of illegal robocalls on its network.

The program includes:

- **Know-Your-Customer (KYC) vetting**
- **Traffic monitoring and analytics**
- **Prohibited-use enforcement**
- **Cooperation with traceback requests**
- **Immediate mitigation and customer suspension procedures**
- **Ongoing compliance audits**

MACS does **not** permit high-risk traffic such as:

- Auto-dialed mass calling
- Lead-generation campaigns
- Caller ID spoofing
- Unlawful telemarketing
- Traffic from unverified entities

4. Know-Your-Customer (KYC) Procedures

MACS employs strict KYC procedures before activating any customer:

4.1 Identity Verification

MACS verifies:

- Legal business name
- EIN or state registration
- Physical address
- Government-issued identification for authorized signers
- Corporate ownership structure

4.2 Service Use Case Review

MACS reviews:

- Nature of the customer's business
- Expected call volume

- Expected call patterns
- Intended use of outbound calling

High-risk use cases are rejected.

4.3 Prohibited Customer Categories

MACS does not onboard:

- Lead-generation call centers
 - Auto-dialer operations
 - Entities engaged in mass cold-calling
 - Entities with prior traceback activity
 - Entities lacking verifiable business identity
-

5. Traffic Monitoring & Analytics

MACS continuously monitors outbound traffic for:

- High-volume bursts
- Short-duration call patterns
- Invalid or unassigned caller IDs
- Repetitive calling to the same numbers
- Known Do-Not-Originate (DNO) patterns
- Traffic inconsistent with the customer's stated use case

MACS uses:

- Upstream carrier analytics
- Real-time alerts
- Automated anomaly detection
- Manual review by compliance staff

Suspicious traffic triggers immediate investigation.

6. Cooperation with the Industry Traceback Group (ITG)

MACS fully cooperates with traceback requests under:

- **FCC 20-136**
- **FCC 21-122**

- **47 CFR § 64.1200(n)**

MACS responds to traceback requests:

- **Within 24 hours**, or sooner when possible
- With complete call records
- With customer identity and use-case information
- With mitigation actions taken

MACS maintains a zero-tolerance policy for customers identified in traceback events.

7. Enforcement & Mitigation Actions

MACS enforces strict compliance with its Acceptable Use Policy (AUP).

7.1 Immediate Actions

Upon detection of suspicious or illegal traffic, MACS may:

- Block the traffic
- Suspend the customer's outbound calling
- Require additional identity verification
- Require call samples or campaign descriptions

7.2 Termination

MACS terminates customers who:

- Originate illegal robocalls
- Engage in caller ID spoofing
- Violate TCPA or FCC rules
- Fail to cooperate with investigations

MACS reports repeat offenders to:

- Upstream carriers
 - The Industry Traceback Group
 - Law enforcement (when required)
-

8. Recordkeeping

MACS maintains:

- Customer onboarding documentation
- KYC verification records
- Call detail records (CDRs)
- Traffic analysis logs
- Traceback correspondence
- Enforcement actions

Records are retained for **minimum 24 months**, consistent with FCC expectations.

9. Upstream Provider Compliance

MACS relies on SkySwitch and its underlying carriers for:

- STIR/SHAKEN authentication
- PSTN interconnection
- Routing
- Numbering
- Call signing and verification

MACS verifies that its upstream providers:

- Are listed in the FCC RMD
 - Have fully deployed STIR/SHAKEN
 - Maintain compliant robocall mitigation programs
-

10. Certification

MACS certifies that:

1. It has implemented a robocall mitigation program designed to prevent the origination of illegal robocalls.
 2. It responds fully and promptly to traceback requests.
 3. It takes immediate action to stop illegal robocalls when detected.
 4. It relies on a fully STIR/SHAKEN-compliant upstream provider.
 5. It files truthfully and accurately in the FCC Robocall Mitigation Database.
-