



Robocall Mitigation Program (RMP)

1. Overview

The filer provides retail VoIP/UCaaS services to end users through a hosted platform. The filer does not operate its own IP-based voice network, nor does it control Session Border Controllers, SIP interconnections, or STIR/SHAKEN authentication systems. All call origination, network-level signaling, and STIR/SHAKEN authentication are performed by the filer's upstream carrier(s). As such, the filer is exempt from STIR/SHAKEN implementation requirements under 47 CFR § 64.6301(a).

2. Basis for Exemption (FCC Rule Citation)

Under 47 CFR § 64.6301(a), the duty to implement the STIR/SHAKEN authentication framework applies only to voice service providers that originate calls on an IP network for which they have the technical ability to authenticate SIP signaling with STIR/SHAKEN.

The filer does not have such technical ability because it does not:

- Operate its own IP voice network
- Control SBCs or SIP interconnects
- Perform STIR/SHAKEN signing
- Possess access to or management of authentication certificates

Therefore, the filer is properly exempt under 47 CFR § 64.6301(a).

3. Robocall Mitigation Practices (Required under 47 CFR § 64.6305(a))

Although exempt from STIR/SHAKEN implementation, the filer maintains and follows a comprehensive robocall mitigation program that includes:



a. Know-Your-Customer (KYC) Requirements

The filer verifies the identity and legitimacy of all new customers prior to activating service. This includes:

- Collecting business information and verifying ownership
- Confirming service use-cases match legitimate business operations
- Screening for high-risk or suspicious traffic patterns prior to activation

Customers with suspicious use cases or insufficient verification are rejected.

b. Ongoing Monitoring and Traffic Analysis

The filer actively monitors customer outbound traffic for:

- Sudden volume spikes
- Short-duration, high-frequency call patterns
- Known robocall or scam signatures
- Irregular call destinations or originating patterns

If suspicious activity is detected, the filer immediately investigates, contacts the customer, and may suspend or terminate service.

c. Cooperation with Traceback Requests

The filer fully cooperates with traceback requests from:

- The FCC
- Law enforcement
- The Industry Traceback Group (ITG)

The filer commits to responding within 24 hours, as required.



d. Enforcement and Remediation

If illegal or suspicious robocall activity is identified, the filer will:

1. Immediately investigate the traffic
2. Suspend or block the problematic call paths
3. Contact the customer to confirm legitimacy
4. Terminate service if misuse is confirmed

The filer maintains a zero-tolerance policy for illegal robocalling.

e. Upstream Carrier STIR/SHAKEN Implementation

All SIP traffic and call authentication is performed by the filer's upstream carrier(s), who have fully implemented STIR/SHAKEN on their networks. The filer relies on this authentication framework, as it does not operate any infrastructure capable of performing STIR/SHAKEN internally.

(This is supported by the SkySwitch guidance email indicating that STIR/SHAKEN obligations are completed upstream.)

4. Summary

The filer is exempt from STIR/SHAKEN implementation per 47 CFR § 64.6301(a) because it does not operate its own IP-based voice network. Nevertheless, it maintains a robust robocall mitigation program, including identity verification, active monitoring, immediate traceback cooperation, and partnered upstream STIR/SHAKEN compliance.

This program ensures that all originated calls are subject to effective mitigation controls consistent with 47 CFR § 64.6305(a).