

Cloud Secure Systems LLC - Robocall Mitigation Program Description

STIR/SHAKEN Exemption

Rule Cited: 47 CFR § 64.6304(a) — Exemption for providers lacking the technical capability to implement STIR/SHAKEN.

Explanation: The filer is a single-owner LLC that resells Grandstream UCM VoIP systems to small businesses. These systems connect to the PSTN via upstream SIP trunk providers who are responsible for STIR/SHAKEN authentication. The filer does not originate calls directly on an IP network and does not have the technical capability to implement STIR/SHAKEN independently. Therefore, the exemption under 47 CFR § 64.6304(a) applies.

Customer Vetting

All customers are vetted prior to activation. This includes verifying business legitimacy, reviewing use cases for outbound calling, and ensuring compliance with anti-spam and robocall regulations.

1. Business Verification:

- Collect and verify business registration documents (e.g., LLC certificate, EIN).
- Confirm the identity of the business owner or authorized representative.

2. Use Case Review:

- Ask the customer to describe how they intend to use the phone system (e.g., customer service, internal communication).
- Evaluate whether the use case aligns with legal and ethical communication practices.

3. Compliance Screening:

- Require agreement to the Acceptable Use Policy (AUP), which prohibits illegal robocalling and spoofing.
- Check against known databases of fraudulent or high-risk entities (e.g., FCC enforcement lists).

4. Onboarding Approval:

- Only activate service after all vetting steps are completed.
- Maintain records of vetting for future audits or investigations.

Traffic Monitoring

Voice traffic is monitored for patterns indicative of illegal robocalling. Alerts are configured to detect high-volume or short-duration call anomalies. Suspicious activity is investigated and service may be suspended if abuse is detected.

1. Call Pattern Analysis:

- Monitor call volume, frequency, and duration.
- Flag patterns like high volume of short-duration calls, calls to known high-risk or international destinations, and sudden spikes in outbound traffic.

2. Automated Alerts:

- Use built-in analytics tools (from the Grandstream UCM or SIP provider) to trigger alerts for suspicious behavior.
- Set thresholds for what constitutes abnormal traffic.

3. Manual Review & Investigation:

- Investigate flagged accounts manually.
- Contact the customer to verify activity if needed.

4. Enforcement Actions:

- Suspend or terminate service if illegal activity is confirmed.
- Report findings to upstream providers or regulatory bodies if required.

Traceback Cooperation

The filer commits to full cooperation with traceback requests from the FCC, law enforcement, and industry traceback consortiums. All requests will be responded to within 24 hours, and relevant call records will be provided to assist investigations.

Company Structure

Principals:

David Parrish, Sole Member and Owner of Cloud Secure Systems LLC.

Affiliates:

None.

Subsidiaries:

None.

Parent Companies:

None. Cloud Secure Systems LLC is independently owned and operated.