

Robocall Mitigation Program Description

Company Information:

- **Company Name:** CallSteward.Com, LLC
 - **FCC Registration Number (FRN):** 0036723716
 - **Point of Contact:** Ed Hills, ed@callsteeward.com.2073432562
 - **Service Type:** VoIP Service Provider (White-Labeled PBX using Bandwidth SIP Trunks)
 - **Exemption Reference:** The filer is exempt from full STIR/SHAKEN implementation under **47 CFR § 64.6301(a)(2)** because it does not originate calls directly to the PSTN; instead, the filer relies on **Bandwidth**, a STIR/SHAKEN-compliant upstream provider, to sign outbound calls on its behalf.
-

Robocall Mitigation Strategies

In compliance with FCC requirements, CallSteward has implemented a comprehensive Robocall Mitigation Program to actively prevent unlawful robocall traffic. The following measures are in place:

1. Traffic Analysis & Monitoring

We actively monitor outbound call traffic to identify and block suspicious patterns that may indicate robocall activity. Our monitoring strategies include:

- Analyzing call volume spikes, unusual call durations, and call patterns that suggest fraudulent activity.
- Implementing **rate limits** and **IP filtering** to restrict suspicious traffic sources.
- Working closely with **Bandwidth** to utilize their fraud detection tools for real-time call analysis and risk assessment.

2. Call Authentication & Identification

To support Bandwidth's STIR/SHAKEN signing process:

- Our PBX systems are configured to insert the appropriate SIP headers such as:
 - **P-Asserted-Identity (PAI)**
 - **Remote-Party-ID**
 - **Identity** header where applicable
- This ensures that Bandwidth can sign outbound calls with an appropriate STIR/SHAKEN attestation level.

3. Blocking Known Robocall Patterns

Our PBX system is equipped with advanced filtering capabilities to:

- Block calls from known robocall numbers.
- Identify and automatically reject suspicious calls that follow fraudulent patterns.
- Maintain an internal **blacklist/whitelist** system for dynamic call control.

4. Traceback Cooperation

CallSteward is committed to responding to **traceback requests** within **24 hours** from:

- The **FCC**

- **Law enforcement agencies**
- **The Industry Traceback Group (ITG)**

We maintain comprehensive records of our traceback activities and cooperate fully with authorities to stop unlawful robocall behavior.

5. End-User Protections

To further protect end-users, we:

- Educate our customers about robocall risks and prevention strategies.
- Provide tools for users to manage call blocking, caller ID filtering, and customized call settings within our PBX platform.
- Employ fraud detection tools to mitigate potential abuse of our network.

6. Reporting and Compliance

- We maintain detailed records of our robocall mitigation efforts, including:
 - Call traffic analysis reports
 - Blocked call records
 - Traceback request responses
- These records are stored securely and retained to meet FCC compliance standards.

Conclusion

CallSteward takes its responsibility to prevent unlawful robocalls seriously. By implementing these comprehensive mitigation strategies and working closely with **Bandwidth** to ensure STIR/SHAKEN compliance, we are committed to protecting our network and end-users from illegal robocall traffic.

We remain fully cooperative with FCC regulations and will continue to enhance our mitigation efforts as needed to maintain compliance and improve our services.