

Robocall Mitigation Program Description

Filer Name: Israel Guadarrama Zarate

Date: 04/06/2026

1. Company Description

Im a reseller of interconnected VoIP services. The company provides voice services to end users but does not own or operate its own telecommunications network infrastructure.

The company relies on its underlying carrier, net2phone, for call transmission, routing, and implementation of network-level services, including STIR/SHAKEN authentication.

2. STIR/SHAKEN Implementation Status

The filer has not implemented the STIR/SHAKEN authentication framework on any portion of its network.

As a reseller, the filer does not originate calls on its own network and relies on its upstream provider to authenticate calls and comply with STIR/SHAKEN requirements.

3. Robocall Mitigation Practices

The filer has implemented a robocall mitigation program designed to prevent the origination and transmission of illegal robocalls. These measures include:

a. Customer Verification (KYC)

The filer performs reasonable due diligence when onboarding customers, including collecting identifying information and verifying the legitimacy of the customer's business where applicable.

b. Terms of Service Enforcement

All customers are required to agree to terms of service that explicitly prohibit the use of the service for illegal robocalling, spoofing, or fraudulent activities.

c. Traffic Monitoring

The filer monitors customer traffic for unusual patterns, including high call volumes, short-duration calls, or other indicators of potential robocall activity.

d. Enforcement Actions

If suspicious or illegal activity is detected, the filer will take immediate action, which may include:

- Investigating the activity
- Suspending services

- Terminating customer accounts
-

4. Cooperation with Traceback Requests

The filer commits to respond fully and within 24 hours to all traceback requests from:

- The Federal Communications Commission (FCC)
- Law enforcement agencies
- The Industry Traceback Group

The filer will cooperate with all such entities to investigate and mitigate illegal robocall activity.

5. Reliance on Upstream Provider

The filer relies on its upstream provider to implement network-level protections, including STIR/SHAKEN authentication and additional robocall mitigation controls.

6. Conclusion

The filer has implemented a robocall mitigation program consistent with FCC requirements under 47 CFR § 64.6305. The filer is committed to preventing the origination of illegal robocalls and will take appropriate actions to ensure compliance with all applicable regulations.