

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN

Company: Ztar Mobile, Inc.

Date: February 25, 2026

Pursuant to 47 CFR § 64.6305, Ztar Mobile, Inc. (“Ztar” or the “Company”) submits this description of its STIR/SHAKEN implementation status and the robocall mitigation procedures it employs to prevent and mitigate illegal robocalls.

Ztar reserves the right to modify, update, or supplement the policies and procedures described herein as necessary to reflect operational, technological, or regulatory developments.

1. Company Background

Ztar Mobile, Inc. operates as a Mobile Virtual Network Enabler (MVNE) providing telecommunications platform and operational support services to Mobile Virtual Network Operators (MVNOs) that offer prepaid wireless voice services to end users.

Ztar does not own, operate, or control transmission facilities, switching infrastructure, or other network elements required to originate calls directly to the public switched telephone network (PSTN).

Instead, Ztar relies on underlying facilities-based carrier partners that provide network connectivity, call routing, signaling, authentication, and network-level robocall mitigation functions.

Because Ztar does not control the underlying carrier network infrastructure, it does not have the capability to independently implement the STIR/SHAKEN call authentication framework.

Services supported through the Ztar platform are primarily intended for consumer and single-line wireless communications, which generally present a lower risk of originating high-volume automated robocall traffic.

Nevertheless, Ztar maintains mitigation procedures appropriate to the risk profile associated with the services supported through its platform.

2. STIR/SHAKEN Implementation

Ztar has not implemented the STIR/SHAKEN call authentication framework and is unable to do so directly.

As an MVNE, Ztar does not control the switching infrastructure necessary to authenticate or sign calls using STIR/SHAKEN.

Consistent with the FCC’s determination in the First Call Authentication Report and Order (FCC 20-42), providers that do not control network infrastructure necessary to implement STIR/SHAKEN may rely on underlying carrier partners to perform call authentication.

Accordingly:

- Calls originating from services supported through Ztar’s platform are routed through underlying facilities-based carriers.
- These carriers implement STIR/SHAKEN authentication for IP-based voice traffic.
- Ztar relies on these carriers to perform call authentication functions.

Ztar complies with applicable FCC robocall mitigation obligations and relies on its underlying carrier partners for network-level call authentication, analytics, and call blocking capabilities.

3. Robocall Mitigation Program

This Robocall Mitigation Plan describes the measures implemented by Ztar to detect and mitigate illegal robocalls associated with services supported through its platform.

As an MVNE supporting MVNO services primarily intended for single-line consumer use, Ztar is not considered a significant source of illegal robocall traffic. Nevertheless, Ztar maintains mitigation procedures designed to address potential robocall risks.

Ztar periodically reviews its mitigation procedures and may update them as necessary to address operational, technological, or regulatory developments.

4. Subscriber Due Diligence

Ztar supports prepaid wireless services through MVNO partners, which maintain the direct retail relationship with subscribers.

Subscriber information available to Ztar may include subscriber identifiers, account data, SIM identifiers (ICCID), device identifiers (IMEI), activation records, or other account-related information made available through the service activation process.

Ztar and its MVNO partners maintain terms of service and acceptable use policies that prohibit unlawful telecommunications activity, including illegal robocalling and fraudulent use of telecommunications services.

Accounts associated with violations of these policies may be subject to restriction, suspension, or termination of service.

5. Downstream MVNO Oversight

MVNO partners supported by Ztar maintain the direct relationship with end users and are responsible for subscriber onboarding, identity verification processes, and enforcement of their respective acceptable use policies.

Ztar requires MVNO partners to maintain policies prohibiting unlawful robocalling and fraudulent telecommunications activity.

Where Ztar becomes aware of suspicious or unlawful activity associated with an MVNO-supported account, the Company may investigate and take appropriate mitigation actions, including restricting, suspending, or terminating services associated with the relevant account or MVNO partner.

6. Fraud Prevention and Activation Controls

Ztar maintains fraud prevention procedures designed to identify potentially abusive or fraudulent activity associated with activations and accounts processed through the Ztar MVNE platform.

These procedures may include automated or manual review mechanisms related to activation patterns, device identifiers (IMEI), SIM identifiers (ICCID), payment indicators, or other signals that may indicate fraudulent or abusive activity.

Where suspicious activity is identified, Ztar may delay or decline activation requests, restrict service capabilities, or suspend accounts associated with the activity.

These measures are intended to reduce the risk of fraudulent use of services supported through the Ztar platform, including potential illegal robocall activity.

7. Traffic Monitoring and Safeguards

Ztar works with its underlying facilities-based carrier partners and MVNO customers to address suspected illegal robocall activity associated with services supported by the Ztar platform.

Because Ztar does not operate switching infrastructure or network-level authentication systems, the Company relies on the monitoring, analytics, and mitigation capabilities of its underlying carrier partners.

If Ztar becomes aware of suspected unlawful robocall activity through notifications from carrier partners, traceback requests, customer complaints, or other credible sources, the Company may investigate the relevant account and take appropriate mitigation actions.

8. Traceback Cooperation

Ztar adheres to industry best practices when responding to traceback requests from the Federal Communications Commission (FCC), law enforcement agencies.

Dedicated Point of Contact

Ztar maintains a designated point of contact responsible for receiving and responding to traceback requests.

Coordination

Ztar coordinates with the FCC, law enforcement authorities, the ITG, and other voice service providers in connection with investigations of suspicious traffic.

Prompt Response

Upon receipt of a traceback request, Ztar will review relevant records and respond within 24 hours of receipt whenever reasonably practicable. If a complete response cannot be provided within that timeframe, Ztar will provide available information and continue cooperating with investigators.

Confidentiality

Information relating to traceback investigations is treated as confidential and disclosed only to the ITG, providers participating in the investigation, regulatory authorities, or when required by lawful legal process.

Ztar maintains records of traceback requests and may review such records to identify accounts associated with repeated inquiries and take appropriate mitigation actions.

9. Reliance on Underlying Carrier Controls

Ztar relies on its underlying facilities-based carrier partners to implement network-level robocall mitigation tools, including STIR/SHAKEN authentication, traffic analytics, and call blocking capabilities.

Because these mitigation systems operate at the carrier network level, Ztar does not independently control or manage these systems.

10. Downstream Provider Responsibility

Ztar provides telecommunications platform services to Mobile Virtual Network Operators (MVNOs) that maintain the direct retail relationship with end users.

MVNO partners are responsible for subscriber onboarding, customer verification, and enforcement of their respective acceptable use policies.

Ztar may investigate and take mitigation actions where suspicious activity is identified; however, responsibility for compliance with applicable telecommunications laws ultimately rests with the service provider maintaining the retail subscriber relationship.

11. Good Faith Mitigation Commitment

Ztar Mobile, Inc. is committed to taking reasonable and good-faith measures to prevent the origination and transmission of illegal robocalls through services supported by its platform.

Where credible information suggests potential unlawful robocall activity, Ztar will work with its MVNO partners, underlying carrier providers, and relevant authorities to investigate the activity and implement appropriate mitigation measures.

12. Registration and Certification

The Company confirms it is registered in the [FCC Robocall Mitigation Database](#) and will keep its registration information updated within 10 business days of any change. The Company will review and recertify its plan annually by March 1.