



ZENTAGE COMMUNICATION

Robocall Mitigation Plan (RMD)

ZENTAGE COMMUNICATION LLC ("ZENTAGE") complies fully with the Telephone Consumer Protection Act (47 U.S.C. § 227) and all applicable FCC rules and regulations. This Robocall Mitigation Plan outlines the proactive measures ZENTAGE has implemented to combat illegal robocalls, fraudulent traffic, and other prohibited activities across its network.

1. Compliance Commitment

ZENTAGE adheres to all requirements set forth by the FCC, including the TRACED Act, and maintains strict operational policies to prevent the origination or transit of illegal robocalls.

2. Filtering & Blocking Tools

ZENTAGE employs multiple filtering mechanisms to detect and block suspicious traffic:

- **SOMOS Real Number System**
- **USTelecom Do Not Originate (DNO) List**
- **YouMail Database Spam Block**

These tools are applied network-wide to mitigate robocall activity as calls traverse the ZENTAGE network.

3. Traceback Cooperation

- Upon receipt of a traceback notice from the USTelecom Industry Traceback Group (ITG), ZENTAGE immediately investigates the reported activity.
- The calling number (ANI) identified in the traceback is blocked without delay.

- ZENTAGE files a response with ITG within **24 hours**, disclosing the source carrier of the activity as required by FCC rules.
- Offending carriers are notified and issued a **first warning** in accordance with ZENTAGE's KYC documentation.

4. Call Blocking Procedures

ZENTAGE performs targeted blocking of ANIs associated with illegal robocall activity. This ensures that fraudulent traffic is removed from the network promptly and prevents recurrence.

5. Designated Point of Contact

ZENTAGE has appointed a single point of contact responsible for handling traceback requests, coordinating investigations, and liaising with law enforcement, FCC, and industry partners.

6. Cooperation with Enforcement

ZENTAGE cooperates fully with law enforcement agencies, the FCC, and the ITG in all traceback requests and investigations.

7. Customer Obligations

- Customers must respond to all traceback requests within **24 hours**.
- Violations of FCC rules or ZENTAGE's Acceptable Use Policy (AUP) may result in suspension or termination.
- Customers found sending illegal traffic forfeit confidentiality protections, and their information will be shared with enforcement authorities and industry partners.

8. Acceptable Use Policy (AUP)

ZENTAGE enforces strict vetting and compliance procedures:

- **First offense:** Written warning.
- **Second offense:** Suspension of service.
- **Third offense:** Termination pending mitigation plan.
- Continued violations result in **immediate and permanent termination**.

9. Know Your Customer (KYC) & Vetting

ZENTAGE requires all customers to undergo a comprehensive vetting process. Verification includes:

1. Business location (must be verifiable).
2. Federal Tax Identification Number (verified via IRS, FCC CORES, USAC).
3. FCC FRN registration (verifiable via CORES).
4. Registration in the FCC Intermediate Provider Registry (IPR).
5. USAC 499A ID (current and verifiable).
6. Registration in the FCC Robocall Mitigation Database (RMD).
7. Full STIR/SHAKEN implementation (verifiable in RMD).
8. Commitment to respond to traceback requests within 24 hours.

Failure to meet these requirements results in denial of service or termination of existing agreements.

10. Contractual Cooperation

All customer agreements include explicit clauses requiring compliance with FCC rules, STIR/SHAKEN authentication, and robocall mitigation practices. Customers must cooperate with ITG and enforcement agencies as a condition of service.