

Robocall Mitigation Database Plan for Telebiz 360

1. Overview and Objectives Telebiz 360 is committed to complying with the Federal Communications Commission (FCC) regulations to mitigate illegal robocalls. This Robocall Mitigation Database Plan outlines the steps, procedures, and technologies employed to identify, block, and mitigate unlawful robocall traffic on Telebiz 360's network. This plan is submitted to the FCC's Robocall Mitigation Database (RMD) in compliance with the February 26, 2024 deadline.

2. Certification Telebiz 360 certifies that:

- All calls originating on our network are subject to a robust robocall mitigation program as outlined in this document.
- Our network complies with STIR/SHAKEN call authentication requirements on IP portions.
- This certification is signed by an authorized officer under penalty of perjury.

3. Reasonable Steps for Robocall Mitigation

3.1 Call Analytics and Blocking Systems Telebiz 360 employs advanced call analytics systems to identify and block illegal robocall traffic. The systems:

- Analyze calling patterns for signs of robocall activity (e.g., high-volume short-duration calls).
- Automatically block calls flagged as unlawful using real-time analysis and known robocall signatures.
- Employ third-party solutions, such as Avaya, to enhance call analytics capabilities.

3.2 Know-Your-Customer (KYC) Procedures Telebiz 360 implements robust KYC protocols to ensure legitimate use of our services:

- Verifies the identity of all new customers during onboarding.
- Includes provisions in customer contracts prohibiting the origination of illegal robocalls.
- Conducts periodic reviews of customer call behavior to detect and address irregular patterns.

3.3 Know-Your-Upstream Provider To mitigate risks from intermediary providers, Telebiz 360:

- Reviews contracts with upstream providers to ensure compliance with FCC robocall mitigation rules.
- Monitors upstream provider traffic for potential sources of unlawful calls.

4. STIR/SHAKEN Implementation Telebiz 360 has implemented the STIR/SHAKEN framework on IP portions of our network to verify caller identity:

- Attaches digital certificates to authenticated calls.
- Rejects unauthenticated calls or marks them as suspicious to downstream providers.
- Regularly updates and maintains STIR/SHAKEN systems to ensure full compliance.

5. Call Traffic Monitoring and Reporting

5.1 Traffic Analysis

- Conducts daily monitoring of traffic patterns to detect anomalies.
- Flags and investigates traffic that matches known illegal robocall characteristics.

5.2 Reporting Protocols

- Reports confirmed instances of illegal robocalls to the FCC and relevant law enforcement agencies.
- Collaborates with downstream and upstream providers to address detected issues.

6. Information Submission to FCC Telebiz 360's submission to the FCC's RMD includes:

- Company identification details (principals, subsidiaries, and affiliates).
- Role in the call chain (originating provider, intermediary, or gateway).
- Confirmation of compliance with STIR/SHAKEN or explanation of exceptions.
- Details of any past investigations related to unlawful robocalls.
- Operating Company Number (OCN).

7. Enforcement and Compliance Measures Telebiz 360 recognizes the enforcement measures outlined by the FCC, including removal from the RMD and financial penalties of up to \$23,727 per violation. To maintain compliance, Telebiz 360 will:

- Periodically audit its mitigation plan.
- Update procedures and technologies to align with evolving FCC guidelines.

8. Conclusion This Robocall Mitigation Database Plan reflects Telebiz 360's dedication to combating illegal robocalls and adhering to FCC regulations. We will continue to monitor, update, and enhance our practices to ensure a secure and compliant communication network.

Stella Edward
 Head Department Sales
 Telebiz 360
 Date: 12/11/2024