

Robocall Mitigation Program Description

1. Program Overview

Our Robocall Mitigation Program aims to reduce the incidence of unwanted robocalls while ensuring compliance with federal regulations. The program is designed to protect our customers from fraudulent and unwanted communications, promoting trust and safety in telecommunications. Our primary objectives include:

- Implementing effective mitigation strategies to minimize robocall impacts.
- Enhancing consumer education regarding robocalls.
- Ensuring compliance with the Federal Communications Commission (FCC) regulations.

2. Risk Assessment

The potential risks associated with robocalls include:

- Increased consumer complaints and dissatisfaction.
- Potential fraud targeting vulnerable populations.
- Regulatory non-compliance leading to fines and reputational damage.
- Erosion of trust in telecommunications services.

3. Mitigation Strategies

To address the risks associated with robocalls, we have implemented the following strategies:

- **Call Endpoint Authentication:** All endpoints with calling capabilities must be authenticated before they can complete calls. Authentication includes UID, secret and IP authentication. In some cases, TLS is implemented which incorporates certificate-based authentication. We do not allow unauthenticated or anonymous calling, and we have no dialer or other machine calling mechanisms within our network. All calls that originate from within our network is from an authenticated human.
- **Federated Networks with IP restrictions:** Integration with external SIP endpoints is implemented in a DNZ zone with IP restrictions in place. IP address of remote endpoints must be explicitly allowed before communication is allowed.

- **Monitoring and Reporting Mechanisms:** We have established a comprehensive call monitoring system to identify and block suspicious call patterns. Additionally, we maintain a reporting mechanism for consumers to report unwanted calls, which are then investigated promptly.
- **Consumer Education Efforts:** We regularly provide resources and information to our customers about robocalls, including how to identify them and report them effectively.

4. Compliance

Our Robocall Mitigation Program complies with federal regulations, including the requirements outlined in 47 CFR § 64.6305. We actively adhere to industry standards for robocall mitigation, ensuring that our program meets all legal obligations.

5. Oversight and Accountability

The implementation and effectiveness of the Robocall Mitigation Program are overseen by our Compliance Officer, who is responsible for ensuring adherence to program policies and procedures. The Compliance Officer reports directly to senior management regarding program status and effectiveness.

6. Evaluation and Reporting

We will evaluate the effectiveness of our robocall mitigation efforts on a quarterly basis. This evaluation will include an analysis of consumer feedback, monitoring data, and the incidence of reported robocalls. Findings will be compiled into a report and submitted to the relevant authorities as required.

7. Updates and Revisions

The Robocall Mitigation Program will be reviewed and updated annually or as necessary in response to emerging threats and regulatory changes. Continuous improvement will be a cornerstone of our approach to mitigating robocalls, ensuring that we adapt to new challenges as they arise.