

Go-Cort, Inc. Robocall Mitigation Program Description

1. INTRODUCTION

Go-Cort, Inc. is committed to addressing the growing issue of illegal robocalls by implementing a robust Robocall Mitigation Program (RMP). This document outlines our policies, processes, and technical measures to ensure compliance with the Federal Communications Commission (FCC) rules regarding robocall mitigation and call authentication frameworks, such as STIR/SHAKEN.

2. OBJECTIVE

The primary objectives of Go-Cort, Inc.'s Robocall Mitigation Program are to:

- Prevent origination and transmission of illegal robocalls on our network.**
- Identify and address patterns of suspicious or fraudulent call traffic.**
- Comply with all FCC regulations and reporting requirements.**

3. SCOPE

This program applies to:

- All voice traffic originated on Go-Cort, Inc.'s network.**
- All interconnected VoIP and other telecommunication services provided to customers.**
- Internal systems and processes used for call verification, authentication, and traffic monitoring.**

4. ROBOCALL MITIGATION MEASURES

To ensure compliance and prevent robocall abuse, Go-Cort, Inc. has implemented the following measures:

4.1 CALL TRAFFIC MONITORING

- Deploy automated systems to monitor call traffic for suspicious patterns, such**

as:

- High call volumes with short durations.
- Repeated calls to invalid or non-existent numbers.
- Use analytics and reports to detect anomalies in traffic behavior.

4.2 CALLER ID AUTHENTICATION (STIR/SHAKEN)

- Go-Cort, Inc. is actively participating in the STIR/SHAKEN framework for caller ID authentication.
- We ensure that all applicable traffic is signed with appropriate attestations:
- A-Level: Full attestation for known and verified callers.
- B-Level: Partial attestation for customers with verified but untrusted origination.
- C-Level: Gateway attestation for traffic passed through external networks.

4.3 CUSTOMER VETTING

- Implement strict processes for onboarding new customers, including:
- Validating identity and business legitimacy.
- Verifying intended use of voice services.
- Conducting ongoing reviews to identify high-risk customers.

4.4 MITIGATION AND REMEDIATION ACTIONS

- If illegal robocall activity is detected, Go-Cort, Inc. will:
- Immediately investigate and confirm the source of suspicious traffic.
- Notify relevant customers and require remediation.
- Suspend or terminate services for customers found engaging in fraudulent activity.

5. COMPLIANCE AND REPORTING

Go-Cort, Inc. adheres to the following compliance standards:

- Maintain records of call verification, authentication, and mitigation efforts.**
- Submit required Robocall Mitigation Program certifications to the FCC's Robocall Mitigation Database.**
- Respond promptly to traceback requests from the Industry Traceback Group (ITG) or regulatory agencies.**

6. PROGRAM MANAGEMENT

6.1 PROGRAM OVERSIGHT

- The Robocall Mitigation Program is managed by Go-Cort, Inc.'s Compliance and Operations teams.**
- Regular program audits and updates ensure continuous improvement and alignment with regulatory changes.**

6.2 TRAINING

- Employees responsible for managing voice services and customer onboarding are trained on:**
 - Identifying illegal robocall traffic.**
 - Following processes for vetting and monitoring.**
 - Implementing mitigation measures and escalation procedures.**

7. CONTACT INFORMATION

For any questions or concerns regarding this Robocall Mitigation Program, please contact:

Go-Cort, Inc.

61149 South Highway 97 #505

Bend, OR 97702

Phone: 888-318-3765

Email: support@apptoto.com

Website: www.apptoto.com

8. CONCLUSION

Go-Cort, Inc. remains committed to combatting illegal robocalls and ensuring compliance with industry standards. Through our Robocall Mitigation Program, we aim to protect our customers, reduce fraudulent activity, and maintain the integrity of our telecommunications network.