

Robocall Mitigation Program Document

Organization Name: Digital Compass LLC

Effective Date: 08/25/2024

Document Version: 1.0

1. Introduction

Objective: The primary objective of this Robocall Mitigation Program is to prevent illegal robocalls from originating or being transmitted through our network. Our commitment is to protect our customers and the integrity of the telecommunications ecosystem by implementing stringent measures to identify, manage, and mitigate unlawful robocall activities.

Scope: This program applies to all voice services provided by Digital Compass across all operational platforms.

2. Commitment to Compliance

Digital Compass commits to full compliance with all applicable laws and regulations pertaining to robocall mitigation, including the requirements laid out in the TRACED Act and FCC regulations. Our program aligns with industry best practices to ensure that we are part of a unified front against illegal robocalls.

3. Detailed Program Description

Analytical Techniques:

- We employ advanced analytics to monitor call traffic patterns and detect anomalies indicative of robocall activity. Our system utilizes AI-driven algorithms to analyze call duration, frequency, and origin to accurately flag potential robocalls.

Authentication and Verification:

- Digital Compass fully implements the STIR/SHAKEN protocol across our network to authenticate and verify the caller ID information, ensuring that the origin of calls can be trusted.

Blocking Strategies:

- We have established criteria for blocking calls that are likely to be illegal robocalls, based on intelligence from analytics, customer complaints, and blacklist data from industry and regulatory bodies.

Robocall Mitigation Program Document

- Calls identified as high-risk are blocked automatically, with immediate notifications sent to the relevant stakeholders.

Monitoring and Oversight:

- Our operations team continuously monitors the effectiveness of our mitigation strategies, adjusting thresholds and parameters in real-time to respond to emerging threats.

4. Ensuring Legitimate Communication

Avoidance of Overblocking:

- Our program includes mechanisms to ensure that legitimate calls are not blocked. This includes a regularly updated whitelist and a robust challenge process where callers can report wrongful blocking.
- We conduct quarterly audits to review our blocking actions and ensure accuracy and fairness in our processes.

Whitelisting Measures:

- Customers and legitimate telemarketers can request to be added to our whitelist by submitting their details through a dedicated portal on our website.

5. Compliance and Collaboration

Adherence to TRACE Act:

- We actively participate in the Industry Traceback Group and comply with all TRACE Act requirements to help trace and block illegal robocalls.

Law Enforcement and Regulatory Communication:

- A dedicated compliance officer is responsible for liaising with law enforcement and regulatory bodies to report and respond to issues related to robocalls.

6. Public and Customer Relations

Point of Contact:

Robocall Mitigation Program Document

- We have established a dedicated email complaints@digitalcompass.com for customers to report robocall incidents or inquire about call blocking and whitelisting.

Consumer Education:

- Regular public awareness campaigns are conducted to educate customers about robocalls and the measures they can take to protect themselves.

7. Record Keeping and Reporting

Documentation:

- Detailed records of all mitigation measures, call analyses, and customer interactions are maintained as per regulatory requirements.
- Annual reports summarizing our mitigation efforts and program effectiveness are prepared and submitted to the FCC.

8. Implementation Plan

Timeline:

- Immediate: Launch of updated analytical tools and public awareness campaign.
- 3 Months: Full implementation of STIR/SHAKEN across all platforms.
- 6 Months: First quarterly audit of call blocking accuracy.