

Robocall Mitigation Plan

Prepared by: Localloop, Inc.

Date: [09/01/2024]

Point of Contact: [Keith Waddell, President, keith@locallooponline.com, 478.453.8324]

1. Introduction

This Robocall Mitigation Plan outlines the procedures and measures **Localloop, Inc.** has implemented to prevent the origination, carrying, and processing of illegal robocalls. In compliance with FCC regulations, including those outlined in FCC Order 24-73, we certify that we are taking all reasonable steps necessary to mitigate illegal robocall traffic on our network. As a gateway provider, we work with our VoIP provider, Telnyx, which provides the STIR/SHAKEN framework for call authentication.

2. Company Information

- **Provider Name:** Localloop, Inc.
- **FRN (FCC Registration Number):** [0028373298]
- **Primary Contact:** [President]
- **Contact Information:** [Keith Waddell, President, keith@locallooponline.com, 478.453.8324]

3. STIR/SHAKEN Implementation Status

As a gateway provider, we rely on Telnyx to provide STIR/SHAKEN call authentication services for the traffic that passes through our network.

- **Status:** Telnyx, our VoIP provider, has implemented the STIR/SHAKEN framework for calls transmitted through their IP-based infrastructure.
- **Partnership with Telnyx:** We ensure that all calls handled by Telnyx are authenticated using STIR/SHAKEN, and we actively monitor the calls passing through our gateway to ensure compliance.

4. Robocall Mitigation Steps

4.1 Call Authentication

Since Telnyx provides the STIR/SHAKEN framework, **Localloop, Inc.** ensures that all calls routed through our VoIP provider are authenticated. For any calls that cannot be authenticated using STIR/SHAKEN, we employ additional verification methods:

- **Verification of Caller Information:** All customers are required to provide accurate and verified caller ID information before they are allowed to send traffic through our gateway.
- **Call Integrity Monitoring:** We monitor the integrity of calls that pass through our network, verifying that they have valid STIR/SHAKEN signatures where applicable.

4.2 Traffic Monitoring

We utilize various technologies to monitor call traffic in real time, ensuring that suspicious patterns or large volumes of calls indicative of robocalling activities are flagged.

- **Analytics-based Monitoring:** We use Telnyx's advanced analytics platform to detect and flag suspicious call patterns, such as high call volumes or calls from unverified sources.
- **Traffic Filtering:** Calls that do not pass STIR/SHAKEN authentication or are otherwise flagged by our monitoring systems are subject to additional scrutiny and may be blocked.

4.3 Call Blocking and Filtering

We employ call-blocking technologies in partnership with Telnyx to prevent the transmission of illegal robocalls:

- **Automatic Call Blocking:** Calls originating from known fraudulent sources or those failing authentication checks are automatically blocked.
- **Real-Time Call Analytics:** Telnyx provides real-time call analytics, allowing us to block or filter calls that are suspected of being illegal robocalls based on established traffic patterns.

4.4 Customer Vetting and Verification

We enforce strict onboarding and customer vetting processes to ensure that all customers using our gateway are legitimate and not engaged in illegal robocalling.

- **Know Your Customer (KYC) Process:** We require thorough documentation from new customers, including valid identification and business verification, before activating services.
- **Ongoing Monitoring:** Active customers are continuously monitored for any unusual calling behaviors. Accounts exhibiting suspicious activity are subject to investigation and possible suspension.

5. Intermediate Provider Controls

As a gateway provider, we take steps to mitigate illegal robocall traffic passing through our network:

- **Traffic Monitoring for Unauthenticated Calls:** In cases where calls originate from providers that do not implement STIR/SHAKEN, we employ alternative traffic screening methods to ensure these calls are legitimate.
- **Collaboration with Telnix:** We work closely with Telnix to ensure that any intermediate providers routing calls through our network meet industry standards for traffic authentication and mitigation.

6. Collaboration with Industry and Authorities

Localloop, Inc. collaborates with other providers and regulatory authorities to share intelligence on illegal robocall activities and coordinate enforcement efforts.

- **Industry Collaboration:** We participate in industry working groups and initiatives such as the Industry Traceback Group (ITG) to help identify and mitigate illegal robocalls.
- **Reporting to Law Enforcement:** When illegal robocall activity is detected, we work with law enforcement and regulatory agencies to report and address these incidents.

7. Employee Training and Awareness

Our employees are regularly trained on our robocall mitigation strategies, including how to identify and report suspicious call traffic.

- **Training Programs:** Employees involved in network operations receive regular training on recognizing robocall patterns and understanding the use of STIR/SHAKEN.
- **Continuous Education:** As technology and regulations evolve, we provide updated training to ensure employees stay informed about new tools and regulatory requirements.

8. Recordkeeping and Auditing

We maintain detailed records of our call traffic and mitigation efforts, ensuring that we comply with FCC regulations.

- **Call Traffic Records:** We keep records of call traffic, including call origin, destination, duration, and authentication status, for a minimum of [X] months.
- **Regular Audits:** We conduct internal audits of our traffic and customer accounts quarterly to ensure compliance with our robocall mitigation policies. Audit results are documented, and corrective actions are implemented as necessary.

9. Future Improvements

We are committed to continuously improving our robocall mitigation efforts, including:

- **Ongoing Partnership with Telnix:** We will continue working with Telnix to explore new technologies and methods for improving call authentication and mitigation processes.

- **Advanced Call Analytics:** We plan to adopt more advanced call analytics tools to better identify and block illegal robocalls.
- **Customer Tools:** We are exploring additional features to provide customers with enhanced tools for managing and reporting suspicious calls.

10. Certification and Plan Submission

As required by the FCC, **Localloop, Inc.** will submit this Robocall Mitigation Plan, along with our certification, to the Robocall Mitigation Database. We are committed to updating this plan and certification as needed to ensure ongoing compliance with regulatory requirements.

Keith Waddell

President

This version now reflects **Localloop, Inc.** as the gateway provider working with Telnyx for the STIR/SHAKEN framework.