

Robocall Mitigation Program Description

Company Name: Avona Technologies LLC

FCC Registration Number (FRN): 0038272258

Overview

Avona Technologies LLC ("Company") operates as a managed service provider (MSP) delivering business telephony solutions utilizing hosted and on-premise PBX systems based on 3CX, in conjunction with Session Border Controllers (SBCs) and third-party SIP trunking providers, including Telnyx. The Company has implemented this Robocall Mitigation Program in accordance with applicable Federal Communications Commission (FCC) rules and guidance to prevent the origination and transmission of illegal robocalls and spoofed caller identification information.

Nature of Service and Role

The Company does not function as a traditional originating or terminating carrier. Instead, it provides customer-managed voice platforms and connectivity configurations, while relying on upstream carriers (e.g., Telnyx) for public switched telephone network (PSTN) access, call origination, and termination. Accordingly, robocall mitigation responsibilities are distributed across the service chain. The Company implements reasonable mitigation controls within its operational scope.

Customer Vetting (Know Your Customer)

The Company conducts reasonable due diligence prior to provisioning telephony services. Such measures include, but are not limited to:

- Verification of business identity, registration, and ownership
- Validation of customer contact information
- Assessment of intended use of voice services
- Evaluation of risk indicators associated with the customer's industry and use case

Customers presenting elevated risk profiles may be subject to enhanced review, restricted service capabilities, or denial of service.

Network Configuration and Controls

Customer telephony environments are provisioned using 3CX PBX systems deployed either in hosted environments or on-premise with dedicated SBC devices. The Company enforces configuration standards intended to reduce misuse, including:

- Authentication controls on SIP endpoints and trunks
- Restrictions on international and high-risk dialing where appropriate
- Segmentation of customer environments
- Controlled provisioning of outbound calling capabilities

Traffic Monitoring and Analysis

The Company monitors customer call activity to identify patterns consistent with illegal robocalling or network abuse. Monitoring includes review of:

- Outbound call volume anomalies
- High call failure or short-duration ratios
- Sequential or predictive dialing patterns
- Activity inconsistent with the customer's stated business purpose

Caller ID Authentication (STIR/SHAKEN)

The Company utilizes SIP trunk providers, including Telnyx, that support STIR/SHAKEN frameworks for caller ID authentication. While the Company does not directly originate calls on the PSTN, it ensures that its configurations do not facilitate caller ID spoofing and relies on upstream providers to apply appropriate attestation levels.

Mitigation and Enforcement Actions

In the event of suspected illegal robocalling or network abuse, the Company reserves the right to take immediate corrective action, including:

- Blocking or restricting outbound call traffic
- Suspending or terminating customer services
- Coordinating with upstream providers to halt traffic
- Reporting activity to appropriate authorities where required

Traceback Cooperation

The Company responds promptly and in good faith to traceback requests from authorized entities, including the FCC and the USTelecom Industry Traceback Group. The Company maintains sufficient call detail records (CDRs) and system logs to support such investigations.

Record Retention

The Company retains relevant records, including CDRs, provisioning data, and customer onboarding documentation, in accordance with applicable legal requirements and industry best practices.

Program Review and Updates

This Robocall Mitigation Program is reviewed periodically and updated as necessary to maintain compliance with evolving FCC regulations and industry standards.

Certification

The Company certifies that it has implemented the robocall mitigation practices described herein in good faith and within the scope of its operations, consistent with FCC requirements.