

YourSIP Telecom

Robocall Mitigation Plan Introduction

Consistent with the rules and regulations of the Federal Communications Commission the following is YourSIP Telecoms Robocall Mitigation Plan. It details our policies and practices to prevent unlawful robocalls from originating on our voice systems. We host VoIP networks and systems that do not have direct access to the PSTN. Our calls are routed to and from our wholesale CLEC that handles all our origination and termination on the PSTN.

Our Mitigation Plan will be broken down into the following sections:

- Customer Onboarding and best practices
- Monitoring outbound Network traffic
- Device and Network Security
- Suspicious call investigation
- Traceback and Enforcement Cooperation

Our onboarding procedure requires our sales team to get a signed Letter of Authorization that includes the client's physical business address, contact person's legal name, federal tax ID and all phone numbers owned by the client. The account managers then cross-reference existing phone bills to verify these numbers. We have multiple interactions with the client to include onsite surveys by experienced technicians to examine the client's infrastructure and the nature of the customer's business. During our installation we instruct and provide the web link to end users on the FCCs best practices to stop unwanted robocalls and texts.

We implement policies and procedures governing the analysis and monitoring of our outbound voice traffic. Consistent with Anti-Robocall Principles for Voice Service Providers, we analyze voice network traffic originating from our systems to identify patterns consistent with illegal robocalls. We have systems in place and thresholds configured that alert us if it detects these patterns. This includes but is not limited to rapid bursts of high call volume, exceeding allowable calls per second rate, total active calls exceeding our normal/average volume, and high call volume from a single number within a specified period.

Our systems are configured to alert us after the allowable registration attempts have been reached. We have the Security Updates enabled to automatically update. We perform port scanning of routers and firewalls, verify firmware is up to date, strong passwords are being used, all default passwords have been changed, any ports being forwarded to devices are disabled if not needed, and that no viruses or malware is running on clients' workstations. We verify our phone systems have their firewalls running with Intrusion Detection enabled. That Operating Systems is up to date, fixes and patches applied, network settings configured with allowable and blocked Ips, thresholds of allowable attempts then blocked if exceeding these thresholds. Our systems notify our tech teams via email and sms when these thresholds are reached. We have a dedicated team that tests our systems for vulnerabilities.

Our technicians are required to obtain the minimum certificates of Network+ and Security+. We update our policies and procedures as needed and when required. We promote continual education and training for our employees and payment reimbursement for testing. We assist the client in best practices. For our jobs where the client does not have an IT Team, we install our own routers and firewalls and when possible we separate the voice and data network enforcing strict password and encryption.

If we are alerted of possible suspicious calling patterns within our systems, we will immediately investigate the call traffic in question. Our team will verify and determine if the activity is malicious and if so, find the root cause and source of this activity. If found to be originating from a clients network we will notify the customer and advise them on mitigation steps to cease or mitigate the calls in question. We have the right to terminate a customer in instances where they are not complaint within acceptable use. If found to be originating from our systems then we will shut down the outbound routes 7, 10, 11 digit dialing on that specific PBX until the issue is resolved.

Consistent with the FCC rules and regulations, YourSIP Telecom will respond fully and in a timely manner to all call traceback requests from the Commission, law enforcement, and the industry Traceback Group, and will cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls.

See below for our dedicated team member that is responsible for addressing our robocall mitigation related issues.

Jason Koster
Owner
35095 US Hwy 19 N #201, Palm Harbor, FL 34684
727-450-8200
support@yoursip.com

YourSIP Telecom qualifies for an extension of STIR SHAKEN implementation under 47 C.F.R. CFR 64.6304(a) since we qualify as a small voice service provider with fewer than 100,000 voice subscriber lines