

LivVoIP.com Inc. DBA TELCOG Communications Robocall Mitigation Plan

(Last Updated 4/27/2024)

LivVoIP.com Inc., operating under the name TELCOG Communications (DBA), will be referenced as TELCOG throughout this document. This comprehensive Robocall Mitigation Plan outlines the methods and practices TELCOG Communications employs to prevent the initiation and propagation of illegal robocalls through its network. The plan is structured to align with the regulations stipulated by the Federal Communications Commission (FCC) under **47 C.F.R. § 64.6305**, requiring all voice service providers to implement a robocall mitigation strategy.

Our client's networks do not implement STIR/SHAKEN but our carrier Skytel Communications does. Skytel will not forward traffic which fails any of their STIR/SHAKEN protocols.

We utilize Skytel as our upstream carrier for all originating and incoming calls, a STIR/SHAKEN compliant upstream provider. This partnership ensures that the telecommunications services provided through TELCOG to our end users are secured with the latest in call authentication technologies. We DO NOT receive unauthenticated SIP calls from an originating provider. TELCOG takes these obligations seriously and is dedicated to implementing effective measures that support the FCC's goals, cooperating fully with law enforcement and the Industry Traceback Group (ITG) in tracing and eliminating illegal robocall activities.

I. COMPLIANCE WITH REGULATIONS AND NETWORK ACCESS CONTROL

TELCOG Communications employs a multifaceted approach to ensure full compliance with federal regulations, particularly **47 C.F.R. § 64.6305**. This compliance is integral to our operations and the trust we maintain with our customers. A cornerstone of our compliance strategy involves stringent controls over network access, which significantly reduce the risk of our infrastructure being used for the origination of robocalls.

Network Access Controls:

To safeguard against unauthorized use and to ensure the integrity of our services, TELCOG has implemented robust network access controls. These controls are

designed to meticulously monitor and manage who can access our network, PBX servers and under what circumstances. By controlling access, TELCOG ensures that all traffic passing through its network is legitimate and authorized, thereby preventing the abuse of our services for robocall activities.

These controls include:

Authentication and Authorization: Ensuring that only authenticated users have access to our network. We use advanced authentication mechanisms that verify the identity of our users before granting access. No customer nor outside user has access to provisioning information that would allow them to originate a call. All provisioning information is maintained and monitored by our network administrators preventing any unknown endpoints from existing on our network.

Monitoring and Surveillance: Continuous monitoring of network traffic allows us to detect and respond to suspicious activities promptly. Our surveillance systems are designed to flag unusual call patterns that could indicate robocall activities. Examples of this would be utilizing software extensions that provide the exact amount of communication channels being used at once. Allowing us to flag and report any unusual changes in our network activity. Skyetel also provides live feedback if there is ever any unusual activity so it can be investigated immediately.

Infrastructure Security Measures: Employing state-of-the-art cybersecurity technologies to protect our network from external threats. These measures include firewalls, intrusion detection systems, and encryption technologies that secure the data transmitted across our network.

Through these proactive steps, TELCOG maintains strict control over its network, effectively ensuring that no illegal robocalls can originate from our system. We adhere to all aspects of **47 C.F.R. § 64.6305**, maintaining full compliance and fostering a secure, reliable service environment for all users.

II. TRACEBACK REQUESTS AND COOPERATION

TELCOG Communications is fully committed to collaborating with the FCC, law enforcement, and the ITG in their efforts to trace and combat illegal robocalls. Our commitment is demonstrated through our prompt and thorough handling of all traceback requests. TELCOG has allocated dedicated resources to manage these requests efficiently, ensuring that responses are provided within 24 hours of receipt.

To facilitate this process, TELCOG has appointed a single point of contact for all traceback communications:

Contact Name: Andrew Armenta

Title: Lead Engineer

Phone Number: 562.273.1005

Email Address: andrew.a@telcog.com

III. CUSTOMER VETTING AND IDENTIFICATION PROCEDURES

Preventing illegal robocalls starts with rigorous vetting of customers who subscribe to TELCOG's voice services. Our comprehensive customer identification and vetting process is designed to verify the legitimacy of every customer and to establish a trustworthy service relationship. This vetting process is critical not only for compliance with legal requirements but also for protecting our network from being misused.

Detailed Vetting Procedures Include:

Verification of Customer Information: Gathering and verifying detailed information about each customer, including physical location, contact information, business registration details, and federal tax ID numbers.

Credit and Background Checks: Conducting thorough background checks, especially for commercial customers who may require more extensive service configurations and may pose a higher risk for illegal activities. We require proof of a legitimate business existing before even considering offering our services to a customer.

Contractual Agreements: Enforcing service agreements that explicitly prohibit the use of TELCOG's services for illegal activities, including the origination of robocalls. These agreements provide the legal basis for immediate action should violations occur.

IV. ROBUST MONITORING AND DETECTION STRATEGIES

TELCOG employs advanced monitoring and detection strategies to identify and mitigate potential robocall threats. Our proactive monitoring regimen includes the analysis of call detail records (CDRs) and real-time surveillance of network traffic. These efforts are designed to detect anomalous calling patterns and behaviors that may indicate robocall activities.

STIR/SHAKEN Implementation: All calls routed through our network benefit from the robust caller ID authentication protocols implemented by Skyetel, significantly reducing the risk of caller ID spoofing and associated illegal activities.

Key Components of Our Monitoring Strategy Include:

Real-Time Traffic Analysis: Analyzing voice traffic in real-time to identify patterns consistent with robocall activities, such as high volumes of short-duration calls.

CDR Analysis: Regularly reviewing call detail records to detect irregularities and ensure that all calls are legitimate and in compliance with established patterns.

Anomaly Detection Systems: Utilizing cutting-edge anomaly detection systems that automatically flag unusual call patterns for further investigation.

V. THIRD-PARTY ANALYTICS AND TECHNOLOGY INTEGRATIONS

To enhance our ability to detect and prevent illegal robocalls, TELCOG integrates third-party analytics solutions into its network operations. These solutions provide sophisticated tools and methodologies to block robocalls at their origin and prevent their propagation through our network.

Utilized Technologies Include:

Advanced Call Analytics: Deploying state-of-the-art analytics technologies that assess call patterns and origins to identify potential robocall activities. Large influxes of traffic volumes will be notified to us immediately through these systems with our own services and Skyetel's.

Blacklisting and Whitelisting Capabilities: Using comprehensive lists to block known robocall origins while allowing legitimate traffic from verified sources. All numbers provided to our vetted customers are also secured via a spam rating. Allowing adjustments to be made to prevent any incoming spam calls from even reaching out to users.

Conclusion

Through the implementation of these robust strategies and compliance measures, TELCOG Communications demonstrates its unwavering commitment to preventing illegal robocalls and maintaining the highest standards of network integrity and customer trust. This document serves as a testament to our proactive approach and ongoing dedication to upholding these standards, ensuring that TELCOG remains a reliable and secure provider of voice services to its users and uphold all requirements listed by **47 C.F.R. § 64.6305**.

This plan not only meets but exceeds the requirements set forth by the FCC, providing a comprehensive framework for robocall mitigation that protects our customers and the integrity of the telecommunications ecosystem.

Regards,

Livvoip.com Inc., DBA TELCOG Communications

Lead Engineer

Andrew Armenta

A handwritten signature in black ink, appearing to read 'Andrew Armenta', with a stylized, flowing script.

April 28, 2024