

Convergia Inc.
Robocall Mitigation Plan
(September 2025)

Introduction

This Robocall Mitigation Plan (RMP) details the reasonable steps and actions taken by Convergia Inc. ("Convergia") to mitigate and eliminate illegal robocalling. Convergia has an ongoing commitment to identify and help alleviate illegal robocalling by pre-qualifying prospective customers, monitoring existing customers for traffic patterns indicative of prohibited robocalls, and working with other providers and regulatory agencies in combatting fraudulent voice activity.

Convergia provides wholesale and retail voice services. All calls that originate on its network are subject to a robocall mitigation program. Convergia has fully implemented STIR/SHAKEN and other appropriate robocall mitigation efforts.

The Company is not a foreign voice service provider.

The Company does not sell services to international call originators using North American Numbering Plan Numbers.

Compliance History

In the past two years, the Company (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has not been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

No prior RMD certification has been removed by the Commission. The Company has not been prohibited from filing in the Robocall Mitigation Database by the Commission.

The person within the Company responsible for addressing all robocall mitigation-related issues, is:

Name: Rohit Dharupta

Title: Director of Operations

Department: Operations

Telephone Number: (514) 463 0574

Email Address: rohit.dharupta@convergia.io

STIR/SHAKEN Implementation

Convergia has fully implemented the STIR/SHAKEN authentication framework across the entire IP portion of its network, and all calls it originates are compliant with § 64.6301(a)(1) and (2).

The Company uses a third-party vendor/underlying carrier to sign its calls and has its own token. The Company does use a third-party call analytics vendor (Ribbon).

Traceback Requests

Convergia utilizes the industry-standard Traceback Group Portal to respond to traceback requests and related inquiries. The Convergia Network Operations Center (NOC) reviews call logs and Call Detail Records (CDRs) to analyze call flows and provide the necessary information accordingly. Traceback requests will be responded to in 24 hours.

The Company's contact information to handle traceback requests is:

Name	Title	Contact Info
Rohit Dharupta	Director of Operations	rohit.dharupta@convergia.io
Victor Rodriguez	NOC Manager	victor.rodriguez@convergia.io
Alfredo Pinda	Customer Support Team Leader	alfredo.pineda@convergia.io

Know Your Customer

Convergia maintains strict due diligence protocols to ensure the legitimate onboarding of customers and upstream providers. The vetting process includes verification of business registration, identification documents, physical business location, and the nature of the business and services offered.

Convergia Customer Screening Process:

- Checks against enforcement actions and prior traceback history
- Prohibits customers with unresolved robocall violations
- Requires contractual compliance with FCC and international anti-robocall regulations

Additionally, prospective customers are required to agree to Convergia's strict and comprehensive Acceptable Use Policies (AUP) prohibiting the act of fraudulent voice activity as a condition of doing business with Convergia.

Further, Convergia's AUP requires all customers to comply with applicable laws and regulations – which would include the Telephone Consumer Protection Act and its implementing regulations, the Telemarketing Sales Rule, regulations implementing the FCC's national Do-Not-Call registry, and all other rules and regulations governing the sending of telemarketing calls and/or robocalls.

Telephone Number Validation:

The Company requires retail customers to sign an attestation they have the right to use the telephone number and supply a current bill showing the telephone number is active and assigned to them.

Ongoing Robocall Mitigation

Convergia employs a combination of internal monitoring tools and third-party call analytics solutions for call labeling, reputation scoring, and anomaly detection. This includes the use of Ribbon's industry-standard call analytics platform. Convergia's Fraud Prevention and Network teams are constantly working on improving the tools that can help to prevent and detect any kind of fraudulent traffic and Convergia management will implement such measures and procedures without undue delays.

Convergia's Terms and Conditions allow for the suspension of accounts involved in fraudulent or illegal use of service:

- A fraud investigation team reviews all flagged incidents
- Suspicious traffic triggers prompt engagement with customers and carriers
- Accounts are suspended or terminated if found to originate unlawful robocalls

Convergia regularly engages with its customers and upstream carriers to review their robocall mitigation efforts and STIR/SHAKEN compliance. Entities failing to comply are blocked from sending traffic.

Updating Convergia's RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(d)(5), (e)(5) and (f)(5), Convergia will update its submission in the RMD within 10 business days of any change to the applicable information it must provide and update in the RMD.

The Company's RMP continues to develop as the Company and the industry gain expertise and deploy new robocall mitigation strategies and will be supplemented in future updates.