

Introduction

Resolutions IT Ltd trading as Rejuvenate IT is committed to combating illegal robocalls and complying with all applicable FCC regulations, including 47 CFR § 64.6305.

This Robocall Mitigation Program (RMP) describes the specific policies, procedures, and technologies we employ to prevent the origination of illegal robocall traffic on our network, as well as our commitments regarding traceback, cooperation, and ongoing compliance.

STIR/SHAKEN Implementation Status

The Company is a UK-based voice service provider serving a small number of business customers with limited US calling needs. All US-bound calls are routed via upstream US-based carriers, who are responsible for STIR/SHAKEN authentication.

As a non-U.S. operator, the Company has not filed FCC Form 499 and does not have an Operating Company Number (OCN). The STI Governance Authority (STI-GA) requires that only U.S.-based service providers with a valid OCN and Form 499 registration are eligible to obtain an SPC token necessary for participation in the SHAKEN ecosystem.

Therefore, the Company is not capable of obtaining an SPC token and, pursuant to 47 CFR § 64.6304(b), is exempt from the requirements of 47 CFR § 64.6301 regarding STIR/SHAKEN call authentication.

Nevertheless, the Company maintains a robust robocall mitigation program and complies with all other applicable FCC requirements.

Reasonable Steps to Avoid Originating Illegal Robocall Traffic

The Company takes the following reasonable steps to avoid originating illegal robocall traffic:

Know Your Customer (KYC) Procedures

All new customers are subject to a thorough vetting process, which includes:

- Verification of business identity and registration (e.g. articles of incorporation).
- Collection and validation of contact information and physical address.
- Review of intended use cases for voice services.
- Screening against industry blacklists and enforcement actions.
- Ongoing monitoring of customer traffic patterns for anomalies indicative of robocalling.
- Periodic re-verification of customer information.

B. Upstream Provider Due Diligence

- The Company maintains up-to-date records of all upstream providers.
- We verify that all upstream providers are listed in the FCC Robocall Mitigation Database and have not been de-listed due to enforcement action.
- We require upstream providers to certify their compliance with FCC robocall mitigation requirements.

C. Traffic Monitoring and Analytics

The Company employs internal analytics systems to monitor call traffic for patterns consistent with robocalling, such as:

- High call volumes to a single destination.
- Short-duration calls.
- Calls to known Do Not Originate (DNO) numbers.
- Suspected illegal traffic is subject to immediate investigation and, if necessary, blocking or suspension.

D. Call Blocking and Remediation

The Company blocks calls that are determined, through analytics or traceback, to be robocalls.

Customers found to be originating robocalls are subject to suspension or termination of service.

The Company maintains records of blocked calls and remediation actions.

Traceback and Cooperation Commitment

The Company commits to:

Responding within 24 hours to all traceback requests from the FCC, law enforcement, and the industry traceback consortium.

Cooperating fully with such entities in investigating and stopping any robocallers that use our service to originate calls.

Maintaining a designated point of contact for robocall mitigation and traceback requests.

Regulatory History

In the prior two years, The Company not been the subject of any formal Commission, law enforcement, or regulatory agency action or investigation with findings of actual or suspected

wrongdoing related to robocalls, spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

Ongoing Compliance and Updates

The Company will update its Robocall Mitigation Database filing within 10 business days of any change to the information provided herein.

The Company will review and update this Robocall Mitigation Program at least annually or as required by changes in FCC regulations or industry best practices.

Public Safety Safeguards

VoIP service is operated and provided from the United Kingdom, and is intended solely for business communications by office staff. The service is not marketed, sold, or intended for use as a primary means of emergency calling in the United States, and does not support 911 or US public safety answering point (PSAP) calling. All users are informed that emergency calls should not be placed using this service, and alternative arrangements for emergency calling are required.

While the Company does not block any calls to emergency numbers, our service does facilitate 911 calling in the United States via our Upstream Providers.

We make all reasonable efforts to ensure 911 or US public safety answering point (PSAP) calling is available, that users are aware of these limitations and that our service is not used for emergency communications.

Certification

This Robocall Mitigation Program is certified as accurate and complete by:

- Name: Martin Yelland
- Title: Technical Director
- Address: Unit 9 Castle Parade, Bournemouth, Dorset, BH7 6SH, UK
- Phone: +44 1202 237 275
- Email: opsteam@rejuvenate.it

Appendix: Required FCC Filing Information

- Business Name(s): Resolutions IT Ltd

- Primary Address: Unit 9 Castle Parade, Bournemouth, Dorset, BH7 6SH, United Kingdom
- Other Business Names in Use: Rejuvenate IT
- All Business Names Previously Used: Rejuvenate IT
- Foreign Voice Service Provider: Yes
- Responsible Person for Robocall Mitigation:
 - Name: Martin Yelland
 - Title: Technical Director
 - Address: Unit 9 Castle Parade, Bournemouth, Dorset, BH7 6SH, UK
 - Phone: +44 1202 237 275
 - Email: opsteam@rejuvenate.it
- STIR/SHAKEN Implementation Status: As detailed
 - The Company has not implemented the STIR/SHAKEN authentication framework on any portion of its network
- OCN: Not Applicable