

SINGULARITY ICT LTD.

Robocall Mitigation Program Description

Filed pursuant to 47 C.F.R. § 64.6305

FCC Registration Number (FRN) 0035457480 · Robocall Mitigation Database filing RMD0022078

Filer status: foreign voice service provider · Date of this description: 8 September 2026

This Robocall Mitigation Program Description is submitted by Singularity ICT Ltd., a company incorporated in England and Wales under company number 13042211 (the "Provider"), pursuant to 47 C.F.R. § 64.6305. It sets out the policies, procedures and technical controls by which the Provider avoids carrying illegal robocall traffic, and records the Provider's commitment to respond to traceback requests from the Federal Communications Commission, from law enforcement and from the Industry Traceback Group within 24 hours.

The Provider has sought to describe what it actually operates rather than what a template would suggest. Where a measure is in place today it is described in the present tense and, where it can be counted, it is quantified. Where a measure is a commitment for the future, it is stated as such.

I. THE FILER AND THE NATURE OF ITS NETWORK

The Provider is an international wholesale voice carrier. Its business consists of exchanging voice traffic with other licensed telecommunications carriers. The following characteristics of the Provider's network are material to how its robocall mitigation obligations arise and how they are discharged:

- The Provider has no retail subscribers of any kind, in the United States or elsewhere. It does not sell voice service to consumers, to enterprises or to end users.
- The Provider does not originate calls from end users. Every call it carries is received from a licensed carrier counterparty and handed to a licensed carrier counterparty.
- The Provider carries no telemarketing traffic, no autodialled or predictive-dialler traffic, no contact-centre traffic, and no traffic originated on behalf of third-party calling campaigns. This is a condition of its interconnection arrangements, not merely a description of its current traffic.
- The Provider holds no North American Numbering Plan resources and has no United States operating presence, point of presence or Operating Company Number.
- Traffic destined for the United States is delivered to licensed United States carriers for termination. The Provider does not deliver traffic to United States end users.

The Provider is accordingly a foreign voice service provider within the meaning of the Commission's rules, and its exposure to illegal robocalling is that of an intermediate carrier: it does not create such traffic, and its task is to avoid accepting it and passing it on.

II. STIR/SHAKEN IMPLEMENTATION STATUS, AND THE PATH TO IT

The Provider has not implemented the STIR/SHAKEN caller identity authentication framework on any portion of its network. It states the reason plainly rather than resting on the certification alone.

Participation in STIR/SHAKEN requires a Service Provider Code token issued by the STI Policy Administrator, which in turn requires the applicant to hold an Operating Company Number and to be authorised to obtain North American Numbering Plan resources directly. The Provider is a United Kingdom carrier, holds no NANP resources and no Operating Company Number, and is therefore not eligible to obtain a SHAKEN certificate. It cannot sign the calls it hands to United States carriers, and the great majority of the traffic it carries uses non-NANP numbering to which the framework does not apply at all.

The Provider does not treat that ineligibility as the end of the matter. Its plan of progress is as follows:

- The Provider will not strip, alter or suppress any SIP Identity header present on traffic it receives, and will pass authentication information through unchanged to the receiving carrier wherever its signalling path permits.

- The Provider will review its eligibility for a Service Provider Code token annually, and immediately upon any change in its United States regulatory footing - in particular if it obtains direct access to NANP resources or an Operating Company Number. It will apply for a token within a reasonable period of becoming eligible.
- Pending eligibility, the Provider will discuss with its United States terminating carriers what attestation they are able to apply to traffic received from it, and what information the Provider can supply to support the highest attestation those carriers can properly give.
- In the meantime all traffic the Provider carries is subject in full to the mitigation measures described in sections III to VIII below, which are designed to reach the same outcome by a different route: refusing traffic that carries a calling number which cannot lawfully exist.

III. TRACEBACK REQUESTS

The Provider commits to respond fully to any traceback request received from the Commission, from law enforcement or from the Industry Traceback Group within 24 hours of receipt, and to cooperate with those bodies in identifying and stopping any party using its service to carry illegal robocalls. A single point of contact for traceback requests is named in Appendix A.

The Provider retains call detail records for every call it carries for a period of twelve months, which is the basis on which it is able to answer a traceback. For any call identified in a traceback request the Provider can establish the carrier from which the call was received, the time and duration of the call, the calling and called numbers as presented, and the route by which the call was passed on.

The point of contact named in Appendix A is the Provider's Network Operations Centre, which is the same contact the Provider gives to every interconnected carrier for technical and support matters and which is monitored continuously. A named escalation contact at director level is given alongside it.

Where a traceback identifies a counterparty as the source of illegal traffic, the Provider will raise the matter with that counterparty immediately, will require an explanation and remedial action, and will suspend or terminate the exchange of traffic where the response is inadequate or where the conduct is repeated.

The Provider will include in its carrier interconnection agreements an express obligation on each counterparty to cooperate in traceback and to identify, on request and without delay, the upstream provider or customer from which a suspected illegal call entered its network.

IV. THE PRINCIPAL TECHNICAL CONTROL: NUMBERING PLAN VALIDATION

The Provider's principal robocall mitigation control is a live filter which rejects calls whose calling or called number falls within a range that the national numbering administration of the country concerned has not allocated. A calling number lying in unallocated numbering space cannot belong to any subscriber anywhere; it is, by construction, a forged calling line identity. Rejecting such calls removes a large part of illegal robocalling and caller-ID spoofing at the point of interconnection, without reference to call content and without any inspection of subscriber data.

This is an operating system and not a proposal. The figures below are taken from the filter build of 7 September 2026 and can be reproduced on request:

- 876,953 number ranges held in the filter.
- 205 country codes, covering 286 territories and numbering areas.
- 833,646 of those ranges are unallocated numbering space. These are rejected in both directions - that is, both as a calling number and as a called number. The check on the calling number is the anti-spoofing control.
- 43,307 ranges are allocated but not reachable from outside the country concerned. These are rejected as a called number only, and are declined politely rather than treated as non-existent.

Each range in the filter carries the evidence on which it rests:

- 295,104 ranges are marked as spare, reserved or unallocated by the numbering administration itself, in its own published register.
- 538,507 ranges are derived as the complement of an administration's complete allocation register - that is, the space the administration has published as allocated is subtracted from the space its plan defines, and what remains cannot be in service. This method is applied only where the register is complete and current enough to support it.
- 35,652 ranges are identified by service category, and 7,655 by carrier premium-rate designation.

The filter is maintained by automated retrieval from the numbering administrations themselves. The Provider monitors 238 administrations worldwide and operates 86 automated fetchers against those that publish machine-readable registers. The refresh cadence follows each administration's own publication rhythm - daily for Germany, weekly for France, weekly to monthly elsewhere - so that the filter follows official change rather than ageing against it. Where an administration publishes nothing, the Provider writes to it and asks; it does not guess.

One safeguard governs the whole system and is worth stating explicitly. No range is ever activated in the filter until it has been checked against the Provider's own record of answered calls. Where the Provider's own traffic shows that numbers in a range are in service, the traffic prevails over the publication and the range is withheld. The purpose of the filter is to reject calls that cannot be genuine, and never to block a working telephone.

V. KNOW YOUR CUSTOMER

The Provider's customers are licensed telecommunications carriers. It has no retail subscribers, so subscriber vetting in the ordinary sense does not arise; the corresponding control is the vetting of carrier counterparties before any traffic is exchanged.

Before the Provider accepts traffic from a new counterparty it establishes:

- the legal identity of the counterparty, its country of registration and its company number;
- its registered and trading address, and the identity of the officer signing for it;
- its licensing or authorisation status in its home jurisdiction, and the nature of its business and of the traffic it proposes to send;
- its technical points of interconnection and the numbering resources it is entitled to use.

Every counterparty relationship is governed by a written carrier agreement. The Provider's own form of agreement contains an origin-based routing and calling-number provision and restricts the delivery of premium-rate traffic. The Provider reserves the right in its agreements to suspend or terminate the exchange of traffic where a counterparty sends traffic that is unlawful or that breaches those terms, and it will exercise that right.

The Provider will not knowingly accept traffic from a counterparty whose business consists of originating automated or campaign calling, and does not offer service to call generators, dialler operators or contact centres.

VI. KNOW YOUR UPSTREAM PROVIDER

The Provider maintains a current record of every carrier from which it accepts traffic, together with the nature of that carrier's business, the jurisdiction in which it is established and the network location at which traffic is exchanged. Its immediate upstream providers are listed in Appendix A.

The Provider knows the identity of every carrier that hands it traffic; it accepts none anonymously and operates no open or unauthenticated ingress. Interconnections are established against known signalling addresses, and traffic presented from an address that is not provisioned is refused.

The Provider will include robocall prevention and traceback cooperation obligations in its agreements with upstream carriers, and will treat a counterparty's refusal or persistent failure to cooperate in traceback as grounds for suspension.

VII. ONGOING MONITORING AND MITIGATION PRACTICES

The Provider monitors its traffic continuously and reviews call detail records on a recurring basis for patterns consistent with illegal robocalling. Particular attention is given to:

- sudden or abnormal increases in call volume from a counterparty, and short bursts of high volume;
- high volumes of very short calls combined with a low answer-seizure ratio;
- sequential or systematically incrementing called-number patterns;
- repeated attempts to numbers that are invalid, unallocated or not internationally reachable;
- calling numbers that repeat implausibly across unrelated destinations, or that match the called number;
- traffic offered to destinations or number ranges that the counterparty has no evident commercial reason to be sending.

Where such a pattern is identified the Provider investigates it and contacts the counterparty concerned. Depending on what is found, the Provider may block the calling numbers or ranges involved, require the counterparty to identify the origin of the traffic, suspend the affected route or the interconnection as a whole, and report the matter to the relevant authority.

The Provider operates a calling-number blocking facility in its switching platform, by which individual calling numbers and number ranges identified as abusive can be blocked immediately and permanently across all routes, independently of the numbering plan filter described in section IV.

VIII. GOVERNANCE, RECORDS AND REVIEW

Responsibility for this program rests with the officer named in Appendix A. The Provider keeps records of traceback requests received and answered, of counterparty investigations and their outcome, and of suspensions and terminations made on robocall grounds.

This description will be reviewed at least annually, and in any event upon any material change in the Provider's network, its counterparty base or its status under the Commission's rules. The Provider will update its filing in the Robocall Mitigation Database within the time required by the rules whenever the information in that filing ceases to be accurate.

The Provider certifies that the information in this description is true and accurate to the best of its knowledge and belief.

APPENDIX A

Traceback single point of contact

Contact: Network Operations Centre, Singularity ICT Ltd.

Telephone: +44 7403 815886

Email: noc@singularityict.com

This is the same technical and support contact the Provider gives to every interconnected carrier, and it is monitored continuously.

Escalation and officer responsible for this program

Name: Ralf Koehler

Title: Director, and the Provider's legal compliance contact

Telephone: +41 79 812 7777

Email: ralf.koehler@singularityict.com

Call detail record retention

Twelve months, for every call the Provider carries.

Immediate upstream providers

The Provider exchanges international voice traffic with the following carriers under direct SIP interconnection and written carrier agreement. Both relationships are bilateral - the Provider both receives traffic from and delivers traffic to each of them. Both are established international wholesale carriers of long standing, and neither is a reseller or an aggregator of retail traffic.

iBasis - international wholesale voice carrier, bilateral interconnection.

Operational contact: Support@ibasis.net

Rates and commercial: customerrates@ibasis.net

Quickcom - international wholesale voice carrier, bilateral interconnection.

Operational contact: customercare@quickcomtel.com

Rates: ratenotification@quickcomtel.com

The Provider's own interconnection is presented on signalling address 162.55.15.38. Traffic offered from any address that is not provisioned for a known counterparty is refused at the session border.

Call analytics

The Provider does not currently use a third-party call analytics vendor. The controls described in sections IV and VII are operated on the Provider's own platform against numbering data obtained directly from national numbering administrations.