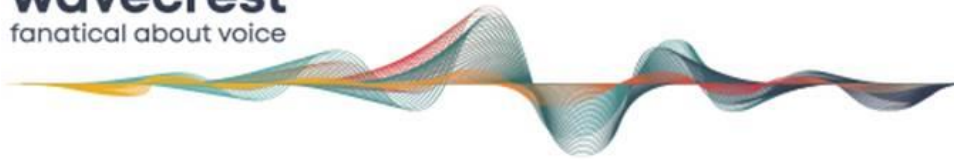


wavecrest
fanatical about voice



RoboCall Mitigation Process

Document History

Version	Version Number	Date	Author	Comment
Draft	0.1	20/04/2021	Kieran Carey	Initial template document
Release	0.2	28/04/2021	Kieran Carey	Initial template document
Revision	0.3	04/04/2024	Kieran Carey	Updated with branding
Revision	0.4	18/04/2024	Graham Packer	Reviewed

Table of Contents

RoboCall Mitigation Process..... 1

Document History 2

Wavecrest’s commitment:..... 3

STIR/SHAKEN:..... 3

Responding to Traceback Requests 3

Wavecrest Approach:..... 3

Stage one -- Proactive Monitoring..... 4

Stage two – Investigation..... 4

Stage three – Response & Mitigation..... 4

Wavecrest's commitment:

- ***Rapid Response*** Promptly addressing Traceback Requests from the Industry Traceback Group (ITG), civil and criminal law enforcement agencies within 24 hours, and actively cooperating in investigations to combat illegal robocalls.
- ***Illegal Traffic Mitigation*** Taking decisive steps to mitigate illegal traffic upon formal notifications from the FCC or other authorized law enforcement agencies.
- ***Robocalling Mitigation*** Enforce comprehensive robocall mitigation measures.
- ***Interconnect Due Diligence*** to ensure all potential customers complete a thorough Know Your Customer (KYC) process and undergo due diligence before onboarding. This critical step ensures the legitimacy and operational integrity of new clients, maintaining network security and regulatory compliance.
- ***Number Validation*** Utilizing our number validator partners to verify the originating and terminating calls through our network.
- ***Regulatory Compliance and Investigations*** Wavecrest is not currently, nor has it ever been, subject to any Commission, law enforcement, or regulatory agency action or investigation related to suspected unlawful robocalling or spoofing activities. This underscores our dedication to lawful and ethical operations within the telecommunications industry.

STIR/SHAKEN:

Wavecrest has not yet upgraded its IP network to implement STIR/SHAKEN. However, it supports Robocall/scam/fraud mitigation through other traffic monitoring practices, as outlined below.

Responding to Traceback Requests

Wavecrest supports the investigation of Traceback requests with defined processes and operating procedure(s). This ensures immediate action upon receiving any trace request from any authorized regulatory body or law enforcement agency including traceback.

Wavecrest Approach:

Wavecrest has implemented the following capabilities within its Network, Business Support System (BSS), and Operating Model:

- Wavecrest operates a 24x7 dedicated fraud team that monitors, detects, and takes immediate action on identified fraud or suspicious traffic. Critically, this team has direct access to the core network and can undertake immediate remedial action if necessary.

- Wavecrest has implemented a strategy that allows per call, Called and Calling party validation. This implementation includes the blocking of 'DNO, invalid, unassigned & Protected' ranges. This strategy has allowed Wavecrest to verify the authenticity of calls in real-time, thereby reducing the likelihood of fraudulent activities and ensuring the integrity of our telecommunications network.
- Wavecrest is an active member of several forums and adopts the best industry guidelines as documented and released by the working groups.
- Wavecrest actively monitors the Telecom and Fraud landscape to ensure we are aware of emerging threats. This information is then used to update or add to our existing rules.

Wavecrest is committed to identifying, where possible, Robocall traffic transiting our network. To achieve this, we have approached it as a three-stage process.

Stage one -- Proactive Monitoring

Near real time traffic analysis using CDR Interrogation and automated alerting to our centralised Networking monitoring platform.

The alerts are based on unexpected calling patterns.

1. large burst of traffic for short durations
2. large volumes of calls from individual CLI's to multiple USA Fixed | Mobile. With low ACD or low ASR.
3. large volumes of calls from multiple CLI's to multiple USA Fixed | Mobile. With low ACD or low ASR.
4. Large volumes of concurrent calls to USA Fixed | Mobile.

Stage two – Investigation

Once suspicious profiles have been identified an investigation will take place to establish the nature and validity of the traffic.

1. Identify the number against our number validator partner(s) databases.
2. Seek to identify if the reported number(s) are routable and dialable.
3. Liaise with the source or destination of the traffic to verify its authenticity.

Stage three – Response & Mitigation

1. Liaise with our customers and Vendor of our findings, requesting their support to authenticate the validity of the reported traffic (this may be initiated as part of the investigation but will continue if further action is required)
2. If agreed, blocking suspect traffic streams on our network either on an IP or CLI | DDI Level.