

Content Guru Inc.

Robocall Mitigation Plan

Content Guru Inc. ("CG") submits this Robocall Mitigation Plan ("Plan") pursuant to 47 C.F.R. § 64.6305(a). This Plan describes CG's efforts to mitigate illegal robocalls consistent with the FCC's rules. CG may modify, add, delete, or otherwise alter any part of this Plan in order to respond to changes in its business, technologies, needs, industry best practices, or any applicable law or regulations. CG will file an updated version of the Plan within ten (10) business days following the date of any changes.

STIR/SHAKEN Implementation Status

CG operates as a voice service provider when it provides voice over internet protocol ("VoIP") services to end-user customers. CG also operates as a non-gateway intermediate provider when it receives calls from originating providers or other intermediate providers and does not terminate such traffic. Except as specifically noted in this Plan, CG undertakes the same mitigation steps (as applicable) when it acts as a voice service provider and a non-gateway intermediate provider.

CG has implemented STIR/SHAKEN Authentication to authenticate all calls that CG originates on its network. In circumstances in which CG's end-user customer engages an alternate provider, CG ensures that the end-user customer has STIR/SHAKEN implemented, either through CG or through the customer's chosen provider.

Terms of Use/Acceptable Use Policies

All end-users are required to adhere to CG's terms and conditions and end-user license agreement ("EULA"), as well as other documentation such as user guides and manuals applicable to CG's service. The EULA authorizes only lawful use of CG's services and details restrictions, including those in relation to automatic dialers and compliance with the Telephone Consumer Protection Act ("TCPA"). CG reserves the right to monitor use of the services and suspend/terminate for any breach of the EULA, or if instructed to do so by the FCC or any other authority.

New and Renewing Customer Vetting Process

CG vets the identity of its subscribers including by collecting the customer's legal name and address, physical location, contact information and the nature of the customer's business. CG will not provide service if a customer's identification cannot be verified.

As part of onboarding a new customer for services provided by CG, a due diligence survey must be completed by the Sales team which is then reviewed and signed off, if approved. An internal customer management system is used to manage this process. The due diligence survey identifies potential signs of fraud that the Sales team should remain aware of when onboarding new customers, including unnecessary urgency on the part of the customer, last minute changes to customer details (e.g., contact numbers, addresses, etc.), and requests for cash payments. The internal process requires the Sales team to validate the customer's business details including the company name, type, company number, and registered address by using publicly available resources provided by U.S. and foreign regulators and/or by verifying the customer's details against the customer's website. The Sales team also is instructed to validate the authenticity of the primary contact for the customer. The internal customer management system directs a Sales team member who has any doubt about the authenticity of customer's business or an individual seeking CG's services to immediately report such concerns.

Upstream Provider Vetting Process

CG has policies and procedures in place to ensure it knows the identities of the upstream providers from which CG accepts voice traffic. For example, before accepting traffic from upstream providers, CG obtains information on an upstream provider's physical address, contact person, state or country of incorporation, federal tax ID (if applicable), the nature of their business, and whether the upstream provider is identified in the FCC's Robocall Mitigation Database. CG only accepts traffic from upstream providers if they have a filing in the Robocall Mitigation Database and that filing has not been de-listed pursuant to an enforcement action. Additionally, CG monitors incoming traffic from upstream providers for signs of potentially illegal robocalls.

CG's supplier terms and code of conduct requires any service provided by a supplier to CG (including the exchange of voice call traffic) to comply with all applicable laws and permits termination of the relationship in the event of any material breach of the terms. The code of conduct further requires all suppliers to implement a management system for carrying out the supplier's responsibilities, including ensuring that the supplier's operations identify and mitigate operational risks related to compliance with applicable legal requirements. Further information on supplier terms and code of conduct can be found here:

<https://www.contentguru.com/en-us/about-us/compliance/>

Network Monitoring, Call Analytics, and Robocall Mitigation

CG invests significant resources to monitor and manage traffic over its network. Automated detection and prevention mechanisms are in place to assist with robocall mitigation.

With the exception of the below third party tools used for monitoring and analytics, the remaining tools are in-house CG developed:

- Oracle Communications Session Border Controller
 - Back to back user agent acting as a boundary for our network
- Splunk
 - For SIEM Monitoring
- ScienceLogic
 - For general monitoring / raising of alarms
 - Otherwise referred to as the Central Monitoring System (CMS)

The details of this are provided below:

Call Analytics

All call-handling nodes generate Call Data Records (“CDRs”), which are automatically imported into a centralized CDR database every 5 minutes. Several automated scripts run against this database to analyze data retrieved from the nodes. These scripts compare the results to established baseline values, and predefined thresholds trigger alarms when anomalies are detected.

Thresholds are tailored based on the severity and nature of the alarm. For example, alarms such as ‘Emergency Services Call Failed’ and ‘Invalid ANI Presented in Call’ are immediately flagged for further investigation. Other alarms, such as increased call counts or specific traffic anomalies, require cumulative data over time to trigger an alert.

Conditions Monitored for Robocall Identification

The following conditions, indicative of robocall or fraudulent traffic, are monitored in real-time and trigger alerts in the Central Monitoring Software (“CMS”), which is actively managed by a 24/7 Network Operations Center (“NOC”) team:

- Drop in Outbound Call Count

- Drop in Inbound Call Count
- Increase in Failed Outbound Calls
- Increase in Failed Inbound Calls
- Increase in Zero-Duration CDRs
- Fraudulent Patterns: Premium Call Duration or Known Fraud Numbers Dialed
- Emergency Services Call Failed
- Invalid ANI Presented in Call
- High Volume of Calls to Invalid Numbers
- High Frequency of Short-Duration Calls for an Organization (Sub-10 Seconds)
- Sequential Numbers Dialed
- Multiple Calls to a Single Destination in a Short Window (e.g., >5 calls in 15 minutes)

The NOC team follows structured Local Work Instructions (“LWIs”) to determine whether the issue lies within a specific node or impacts remote organizations. If localized issues are identified, the team isolates and blocks affected nodes. Due to a platform capacity surplus at all times of over 50%, there is no impact to ongoing services during such maintenance activities.

Robocall Detection and Mitigation Process

The highlighted alarms are critical in identifying robocall patterns, as they align with known robocall behaviors. When such alarms are triggered:

- The NOC team investigates the affected numbers and notifies the respective customers via the Support team.
- Every effort is made to assist customers in identifying and stopping the traffic at their end.
- If the customer is unable to resolve the issue, the NOC team quarantines the associated ANIs to prevent further robocall activity.

Network Monitoring and Infrastructure

On the networking side, CG employs Oracle Session Border Controllers (“SBCs”) to manage call traffic and capacity. All network data is ingested into a centralized SIEM platform. Advanced automation and predefined rules within the SIEM continuously analyze network traffic for anomalies, including:

- Unusual call routing behavior.
- Traffic spikes indicative of robocall campaigns.
- Invalid or spoofed ANIs are also detected and automatically blocked at an application level. Only access numbers owned by the customer can be presented.

When suspicious traffic is detected, alarms are triggered automatically, enabling the NOC team to act swiftly to mitigate risks, block problematic nodes, and maintain the integrity of the platform.

By combining comprehensive CDR analytics, robust network monitoring, and automated alarm systems, we ensure efficient detection, investigation, and blocking of robocall traffic while safeguarding legitimate services for all customers.

Traceback Commitments

CG commits to respond fully, within 24 hours, to all traceback requests from the FCC, law enforcement and the industry traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers that use CG's service to originate, carry, or process illegal robocalls.

Ownership and Management

CG has no subsidiaries. CG is a subsidiary of its Parent company, Redwood Technologies Ltd. The parent company is headquartered in the United Kingdom.

Information regarding CG's leadership team can be found at:
<https://www.contentguru.com/en-us/about-us/leadership/>.

Version Control

Version	Date	Comments
2.0	23-April 2026	STIR/SHAKEN Implementation capability update
1.0		Document creation