

CAMBRIDGE TELECOMUNICAÇÕES LTDA

Plan for the Mitigation of Illegal Automated Calls (Robocalls)

1. Objectives and Responsibilities

1. General Objective

Establish guidelines and measures to prevent, identify, block, and effectively mitigate illegal automated phone calls.

2. Specific Objectives

- Ensure the company's policies and processes comply with current regulations.
- Protect the network infrastructure from abuse and misuse leading to illicit robocalls.
- Provide transparency to regulatory agencies and customers regarding actions taken against fraudulent or illegal traffic.
- Reduce the incidence of illegal automated calls on the network, thereby protecting end users.

3. Responsibilities

- **Compliance/Regulatory Team:** Ensure the plan meets all applicable norms and regulations.
- **Network Security/Operations Team:** Implement and maintain monitoring and call-traffic analysis systems, as well as take blocking or mitigation actions when necessary.
- **IT and Engineering Team:** Develop or integrate tools to assist in identifying suspicious automated call patterns.
- **Commercial/Sales Team:** Validate the legitimacy of new and existing customers, communicating and enforcing acceptable use policies.

2. Control Measures for New Customers

1. Registration and Verification Process (KYC – Know Your Customer)

- Require official documentation and identity verification for individuals or legal entities before enabling voice service.
- Perform cross-checking of customer data using public or private databases (where permitted by law).
- Require signing a Terms of Use agreement explicitly banning illegal automated calling practices.

2. Initial Traffic Limitation

- Set call limits and monitor call volume and dialing patterns for the customer during the first days/weeks of service.
- Gradually increase these limits as legitimate usage history is established.

3. Education and Guidance

- Provide clear information to customers about illicit automated calling practices and the contractual and legal consequences.
- Maintain support channels for clarifying acceptable use.

3. Control Measures for Existing Customers

1. Continuous Monitoring of Call Patterns

- Implement real-time or near real-time analysis systems to detect abnormal traffic spikes and suspicious patterns (very short calls, high call-per-minute rate, dialing to blocked/repeated numbers, etc.).
- If potential illegal robocalls are detected, suspend or temporarily limit the call traffic from that customer and initiate an internal investigation.

2. Periodic Auditing

- Conduct random and periodic checks of call volume, destinations, and success/failure rates.
- Review configurations of accounts with high call volumes to ensure adherence to acceptable use policies.

3. Alert and Rapid Response Mechanism

- Configure automated alerts to notify the responsible team whenever predefined thresholds are reached (e.g., x calls per second, y consecutive short calls, z calls to invalid numbers).
- Enable instantaneous blocking of suspicious traffic until the legitimacy of the calls is confirmed.

4. Identification, Blocking, and Investigation of Illegal Traffic

1. Blocking Procedure

- When clear patterns of illegal automated calls are identified, initiate preventative blocking of routes or the customer itself.
- Immediately notify the responsible customer (when precisely identifiable) of the blockage and provide a timeframe for clarification.

2. Internal Investigation

- Activate a specialized team to analyze call logs and network records.
- Check for any recurrences or evidence of bad faith by the customer.
- Document the entire investigation process, including date, time, call volume, and concluding report.

3. Escalation and Communication with Authorities

- If signs of criminal activity are detected or if there is a legal obligation, notify the competent authorities.
- Maintain detailed records to facilitate enforcement and investigation by regulatory agencies.

5. Transparency and Reporting

1. Uploading the Mitigation Plan

- Make this Robocall Mitigation Plan available to regulatory agencies as required, updating it whenever significant changes occur.

2. Regular Reports

- Provide reports when spam is detected, volume of blocks performed, number of open and closed investigations, etc.
- Share aggregated incident information with the regulator to improve fraud detection on an industry-wide level.

3. Privacy Policy

- Ensure monitoring and analysis actions comply with data protection and privacy legislation, informing users about call data (metadata) collection and handling practices.

6. Continuous Updates and Training

1. Updating Tools and Policies

- Keep call analysis tools up to date to address emerging trends and new fraud techniques.
- Review and update this plan periodically (at least annually) or whenever regulatory changes occur.

2. Team Training

- Provide training for technical, support, and sales teams to ensure understanding and adoption of illegal call mitigation practices.
- Disseminate knowledge about identifying suspicious patterns and escalation workflows.