

Rysedorph IT Inc has implemented robust policies and practices to prevent the origination of illegal robocalls, including:

- **Traffic Monitoring and Analytics:** All voice traffic is continuously monitored using automated tools to detect unusual calling patterns, high call volumes, or other indicators of potential robocalls.
 - **Customer Vetting:** All customers are subject to a strict onboarding process that includes verifying their business identity, understanding the nature of their use case, and requiring compliance with all FCC rules and applicable laws.
 - **Call Authentication:** Calls originating from our platform utilize the STIR/SHAKEN framework to ensure proper call authentication and reduce spoofing.
-

2. Call Authentication Practices

- Rysedorph IT Inc works with Bandwidth, our upstream carrier, to implement the STIR/SHAKEN framework.
 - All calls are signed with appropriate certificates to validate the originating number. Calls received from Bandwidth are verified before being passed to the destination.
 - Non-IP-based calls or calls that cannot be authenticated using STIR/SHAKEN are subject to alternative mitigation measures, such as real-time traffic analysis.
-

3. Mitigation of Calls Not Fully Authenticated

- Calls that are not fully authenticated (e.g., from legacy networks) are analyzed for patterns indicative of robocall activity. Calls flagged as suspicious are either blocked or subject to additional scrutiny before completion.
 - Reports are generated regularly, and flagged calls are reviewed by our compliance team to prevent potential abuse.
-

4. Collaboration with Industry Initiatives

- Rysedorph IT Inc participates in industry forums and collaborates with organizations like the Secure Telephone Identity Governance Authority (STI-GA) to advance the adoption of robocall mitigation standards.
 - We also adhere to best practices outlined by the FCC and industry experts to continuously improve our mitigation practices.
-

5. Consumer Education and Support

- We provide educational materials to our clients regarding the dangers of robocalls and the importance of compliance.
 - Our customer support team is trained to handle reports of suspected robocalls and assist clients in mitigating abuse of their accounts.
-

6. Regular Auditing and Reporting

- Our robocall mitigation practices are reviewed quarterly to ensure compliance with FCC requirements.
 - Detailed logs of all flagged traffic and mitigation actions are maintained for at least two years and are available for inspection upon request by the FCC.
-

Certification:

Rysedorph IT Inc certifies that it has implemented the practices described above and will comply with all applicable FCC rules and regulations under 47 CFR § 64.6305.