

Ace Peak Invest Pte Ltd – Robocall Mitigation Policy

Ace Peak Invest Pte Ltd is a foreign interconnected voice provider that carries or processes calls using North American Numbering Plan (NANP) resources. As a non-gateway intermediate provider, we implement this robocall mitigation program to comply with 47 CFR § 64.6305(f) and prevent the carrying or processing of illegal robocall traffic. Our program includes reasonable, multi-layered steps to avoid carrying or processing unauthorized robocalls, coupled with full cooperation in traceback and enforcement efforts.

1. Upstream Provider Verification and Know-Your-Upstream-Provider (KYUP) Procedures

We require all upstream providers—new and renewing—to provide website details, KYUP documentation (e.g., government-issued identification, business registration), and other relevant information. All submissions are thoroughly verified against government databases and third-party sources to confirm authenticity and legitimacy. For new upstream providers, we conduct enhanced due diligence, including review of business purpose and traffic patterns prior to acceptance. Renewing upstream providers undergo annual compliance re-verification.

2. Signed Agreements and Contractual Obligations

All upstream providers must sign a formal agreement affirming they are legitimate entities and will not transmit illegal robocalls. The agreement includes contractual provisions prohibiting unauthorized traffic, requiring compliance with FCC rules (including STIR/SHAKEN where applicable), and mandating immediate reporting of suspected violations. Upstream providers must maintain a functional domain with an operational website. Violations trigger immediate suspension.

3. Blocking Invalid Traffic and DNC Compliance

Our systems block all invalid traffic. Do Not Call (DNC) compliance is enforced network-wide to prevent unauthorized calls to registered numbers where applicable.

4. Call Analytics and Spam/Spoofing Detection

We utilize in-house call analytics systems for real-time pattern recognition, anomaly detection, and behavioral analysis. These systems generate daily reports to identify and track spam and spoofed calls. Any ANI flagged as spam or involved in suspicious activities is promptly blocked. (No third-party analytics vendors are currently used; all processing is internal.)

5. Zero Tolerance for Repeated Violations

Upstream providers persistently engaging in spoofing or robocall activities are permanently blocked from our network following investigation.

6. Compliance with USA Traceback Consortium

We fully cooperate with the USA Traceback Consortium. Traceback requests from the FCC, law enforcement, or the consortium are responded to within 24 hours. We work closely with upstream providers to identify and address sources of unauthorized calls.

7. Enhanced Monitoring and Proactive Measures

Systems are continuously monitored for unusual call patterns (e.g., high-volume short-duration calls, rapid ANI changes). Alerts trigger immediate review and potential blocking of potential robocall traffic.

8. Strict Policies for High-Risk Traffic

We enforce stringent controls on high-risk routes, including dynamic blocking based on behavior analysis, volume thresholds, and complaint data.

9. Regular Training and Updates

Our teams receive regular training on the latest robocall prevention techniques, FCC regulations, and industry best practices.

10. Upstream Provider Education and Awareness

We actively educate upstream providers on FCC regulations, compliance obligations, and consequences of transmitting unauthorized traffic to promote responsible usage.

11. Audit and Review Processes

Regular audits of traffic, compliance protocols, and mitigation effectiveness are conducted to ensure adherence to our policies and FCC requirements.