

Pursuant to 47 C.F.R. § 64.6305, CommPeak Limited, having its registered office at 1003 Centre Point, 181-185 Gloucester Road, Wan Chai, Hong Kong, Hong Kong (hereinafter: "**CommPeak**") submits this Robocall Mitigation Plan.

CommPeak's Robocall Mitigation Plan delineates the company's policies and procedures to minimize or eliminate outbound illegal robocalls and the current status of its STIR/SHAKEN implementation. CommPeak considers these practices and procedures as constituting reasonable steps to prevent the origination of illegal robocalls. Furthermore, it assures its commitment to respond to traceback requests from the Industry Traceback Group (ITG), the FCC, and law enforcement agencies. CommPeak reserves the right to amend, modify, or delete any of the policies and procedures described in the plan to align its business, capabilities, and requirements with the dynamic and evolving industry standards.

CommPeak certifies that:

Service Classification:

CommPeak Limited operates as a VoIP service provider and reseller, providing services to:

End users; and Business customers, including resellers and smaller telecommunications providers CommPeak does not primarily originate retail consumer traffic at scale, but may:

Facilitate transmission of voice traffic from customers;

Act as an intermediate provider in certain call paths

CommPeak does not knowingly act as a gateway provider for illegal robocall traffic into the United States and has implemented safeguards to prevent such use.

It has implemented a robocall mitigation program reasonably designed to prevent the origination and transmission of illegal robocalls, including those introduced by downstream customers;

It takes affirmative, risk-based steps to prevent its network from being used as a conduit for illegal robocalls;

It responds to traceback requests promptly, completely, and within required timeframes (including within 24 hours where applicable);

The information contained herein is true, accurate, and complete.

STIR/SHAKEN Implementation Status:

CommPeak's current status with respect to STIR/SHAKEN implementation is as follows:

- ☐ My traffic is fully attested.
- ☒ My traffic is partially attested.
- ☐ None of my traffic is attested yet

Implements STIR/SHAKEN authentication where technically feasible;

Assigns attestation levels based on the degree of customer verification;

Applies robust non-STIR/SHAKEN mitigation measures for all unauthenticated traffic.

CommPeak has a subscriber base of fewer than 100,000. Consequently, the company is dependent on the ongoing extension from the STIR/SHAKEN implementation provided to small carriers under 47 CFR § 64.6305 to ensure the completion of the STIR/SHAKEN technology implementation. It is worth noting that all calls originating from CommPeak's network must adhere to the policies and procedures set out in this Robocall Mitigation Plan. These policies and procedures are intended to prevent the use of CommPeak's services to originate unlawful robocalls.

Risk-Based Robocall Mitigation Framework

CommPeak applies a risk-tiered compliance model, reflecting its role as a reseller and service provider to smaller entities.

Customer Vetting and Onboarding Controls

CommPeak performs Know Your Customer (KYC/KYB) procedures, including:

Verification of legal identity and incorporation details;

Validation of business activities and intended traffic use;

Collection of beneficial ownership and contact information (where applicable);

Screening against fraud and abuse indicators.

For reseller and provider customers:

Confirmation of their own robocall mitigation practices;

Requirement to comply with applicable FCC obligations (where relevant);

Contractual obligation to prevent illegal robocalls downstream.

Contractual and Policy Enforcement

All customers are bound by:

Terms of Service

Acceptable Use Policy (AUP)

Service Agreements

These include:

Explicit prohibition on illegal robocalls and spoofing;

Requirement for valid caller ID usage;

Immediate enforcement rights, including:

Traffic blocking

Suspension

Termination without notice in high-risk cases

Traffic Monitoring and Active Mitigation

CommPeak operates continuous, multi-layered traffic monitoring, including:

Analysis of Call Detail Records (CDRs);

Short-duration/high-volume patterns;

Abnormal Answer-Seizure Ratios (ASR);

Repetitive dialing patterns.

CommPeak may, without prior notice:

Block specific traffic streams;

Throttle or rate-limit traffic;

Suspend or terminate accounts;

Require customer remediation within defined timeframes.

Caller ID and Telephone Number Validation

CommPeak enforces strict caller ID integrity requirements:

Customers must demonstrate valid right to use telephone numbers;

Numbers are validated through:

Internal systems;

Industry-standard validation tools.

CommPeak prohibits spoofing or misleading caller ID usage;

Blocks traffic where caller ID cannot be reasonably validated;

Investigates discrepancies between caller identity and customer profile.

Upstream and Downstream Provider Controls

Upstream Providers:

Engages only with reputable upstream providers;

Requires contractual compliance with anti-robocall obligations;

Monitors upstream traffic integrity.

Downstream Customers (Resellers / Providers):

Downstream providers must implement their own robocall mitigation programs;

CommPeak may request evidence of compliance;

Traffic from downstream providers is treated as high-risk by default.

FCC RMD Awareness, where applicable, CommPeak:

Verifies whether interconnected providers in the call path are listed in the FCC Robocall Mitigation Database;

May restrict or block traffic from providers that fail to demonstrate compliance.

Traceback Readiness and Response

CommPeak maintains a formal traceback response program, including:

Dedicated compliance personnel;

Internal escalation procedures;

Ability to identify the immediate upstream and downstream source of traffic.

Commitments:

Response to traceback requests within 24 hours or sooner;

Provision of accurate and complete information;

Cooperation with:

Industry Traceback Group (ITG)

FCC

Law enforcement

Contact: abuse@commpeak.com

Anti-Gateway Abuse Safeguards

Recognizing regulatory focus on gateway providers, CommPeak:

Implements controls to prevent its network from being used as an entry point for illegal robocalls into the United States;

Monitors international traffic for U.S.-bound routing risks;

Applies heightened scrutiny to cross-border traffic flows.

Recordkeeping and Audit

CommPeak maintains:

Customer onboarding and verification records;
Traffic monitoring logs and alerts;
Traceback request logs and responses;
Enforcement action records.

Periodic internal reviews are conducted to:

Assess effectiveness of mitigation measures;
Identify emerging risks;
Enhance controls.

Continuous Improvement

CommPeak continuously:

Updates its mitigation practices;
Adapts to evolving FCC guidance and enforcement trends;
Enhances detection and blocking capabilities.

Statement of Responsibility

CommPeak acknowledges its responsibility as a VoIP provider and reseller to:

Prevent the misuse of its network;
Actively mitigate illegal robocalls;
Ensure compliance across its customer base and traffic flows.