

INSPAY PAYMENT NETWORK PRIVATE LIMITED

Robocall Mitigation Plan

INSPAY PAYMENT NETWORK PRIVATE LIMITED is engaged in telecommunications services, purchasing communication minutes from global providers and reselling them to customers. This Robocall Mitigation Plan is submitted pursuant to 47 C.F.R. § 64.6305 to describe our implementation of the STIR/SHAKEN framework and the measures we employ to prevent and mitigate illegal robocalls.

STEPS TAKEN TO PREVENT ILLEGAL ROBOCALLS

Customer Documentation:

We collect proof of identity and address during customer onboarding, with agreements clearly outlining acceptable use of our platform.

Illegal Robocall Mitigation:

We utilize advanced analytics to detect patterns such as short-duration, high-volume calls or repetitive calling to the same destinations. Suspicious cases are escalated to carriers for verification, with temporary blocking enforced if necessary.

Industry Cooperation:

We fully participate in traceback efforts and respond to law enforcement within 48 hours. We also maintain CLI verification using Call OTP authentication to ensure legitimacy.

STIR/SHAKEN Implementation:

Our network is capable of passing STIR/SHAKEN tokens without alteration. ANI blacklists and Do Not Call (DNC) blocks are in place to curb unlawful traffic.

CUSTOMER DUE DILIGENCE

Spam Filtering:

- Spam Scout Filter: Continuously updated algorithmic filtering to stop spam/scam calls.
- IPQS Premium Filter: External real-time filtering database for enhanced protection.

KYC Verification:

- Performed via Stripe and other compliance platforms.
- Company registrations cross-checked for legitimacy.

Real-Time Transcription Analysis:

- Class 4 transcription analysis identifies robocall campaigns without recording audio.
- Customers flagged must provide consent for enhanced fraud detection.

CUSTOMER OBLIGATIONS

- Customers are educated on telecom security, safety, and fair usage policies.
- Signing of an undertaking acknowledging compliance obligations.
- Non-compliance results in suspension and potential reporting to authorities.
- Malicious activity requires customer consent for call recording and further analysis.

CONTRACTUAL SAFEGUARDS

Spam Filtering Clause: Customers agree to implementation of Spam Scout and/or IPQS filters.

KYC Compliance Clause: Customers consent to KYC checks through Stripe or other providers.

Safety and Security Undertaking: Customers confirm their understanding of telecom obligations.

Consent for Call Recording: Customers acknowledge consent for call recording when fraud is suspected.

MONITORING & RESPONSE

Automatic Monitoring:

- Real-time spam filters and transcription analysis.
- Alert system triggers management review for abnormal activity.

Manual Checks:

- Periodic KYC updates and manual reviews of flagged accounts.

Automated Actions:

- Temporary suspension of traffic or accounts.
- Issuance of warnings or investigation notices.

Trigger Points:

- Suspicious activity detection.
- Non-compliance with telecom obligations.
- Regulatory changes requiring compliance updates.

TRACEBACK COMPLIANCE

Our internal monitoring system identifies suspicious outbound traffic and alerts us when calls originate from invalid, unallocated, or poor-reputation numbers. Suspected unlawful calls are investigated immediately. Accounts found in violation may be warned, blocked, or terminated.

We cooperate fully with the FCC, law enforcement, and the Industry Traceback Group (ITG). All traceback requests are investigated within 48 hours, and we aim to integrate with ITG for faster response times.

For further information or assistance, please contact:

Email: amritpal.malik@inspaycomm.com