Objective and Scope The objective of NSG NETWORKS Robocall Mitigation Plan is to prevent illegal robocalls from originating or passing through our network. This plan outlines specific policies, procedures, and technical measures that comply with the Federal Communications Commission (FCC) requirements. Our proactive approach includes monitoring, identifying, and mitigating suspicious traffic while fully cooperating with industry traceback initiatives. This plan applies to all VoIP and telecommunications services provided by NSG NETWORKS . Robocall Mitigation Procedures as an Originating Provider A. Use Policy (Website Terms & Conditions) NSG NETWORKS enforces strict Acceptable Use and Anti-Fraud Policies published on our website. These policies ensure that customers are aware of prohibited behaviors and illegal activities, including:

• U sing services for robocalling, auto -d ialing, telemarketing without consent, or other illegal purposes.

• Reselling or rebilling our services without authorization.

• Spoofing caller ID or engaging in fraud. Violations of these terms result in suspension or termination of service. B. Know Your Customer (KYC) Protocols To prevent unauthorized or fraudulent use of our network, we enforce stringent KYC protocols to verify the identities of all new customers:

• For Individual Customers: Verification includes a valid government -i ssued ID (e.g., driver's license or passport) and proof of address, such as a utility bill.

• For Business Customers: We verify business documentation (e.g., certificate of incorporation, tax ID) and perform due diligence, including check ing the business website, physical address, and a verifiable company contact email. C. Contractual Terms Our contracts contain provisions to ensure compliance with local and federal laws, including clauses prohibiting number spoofing, robocalling, or any i llegal activity. NSG NETWORKS reserves the right to suspend or terminate service upon discovery of any violations. III. Robocall Mitigation Procedures as an Intermediate Provider For traffic exchanged with third- party providers, we require identity v erification and enforce contract terms to prevent illegal robocalls. Our agreements with intermediate providers include:

• Cooperation with fraud prevention and mitigation efforts.

• Compliance with FCC and industry regulations.

• Provisions allowing audit and monitoring of call detail records to detect and prevent illegal robocalls.

IV. Robocall Mitigation Procedures as a Gateway Provider NSG NETWORKS applies the same standards and contractual requirements to gateway providers as we do for intermed iate providers. These

agreements include:

• Data sharing provisions for fraud detection and traceback requests.

• Suspension of services if providers fail to meet anti-f raud standards or regulatory requirements.

• Mandatory cooperation with law enforcement investigations related to illegal robocall activities.

V. General Robocall Mitigation Procedures A. Monitoring and Traffic Analysis NSG NETWORKS uses a 24/7 monitoring system in our Network Operations Center (NOC) to detect suspicious traffic patterns, including:

• High volumes of short-duration calls.

• Spoofed or fraudulent numbers.

• Abnormal call termination patterns. Our system also includes third-party fraud detection tools that monitor, flag, and block potential robocall activity in real time. B. Investigating and Responding to Suspicious Activity Upon detecting suspicious traffic, our fraud team investigates the details to confirm whether illegal robocalling activity is present. Alerts are generated and reviewed, and if necessary, services are suspended or terminated to prevent further illegal activity. NSG NETWORKS participates actively in traceback initiatives with the Industry Traceback Group (ITG) and responds to all law enforcement and industry requests within 24 hours. C. Suspension and Mitigation of Illegal Traffic If illegal traffic is confirmed, NSG NETWORKS will immediately suspend the related services following regulatory guidelines. Customers are notified, and further actions may be taken to prevent recurring violations. D. Industry Collaboration NSG NETWORKS is committed to collaborating with industry groups to stay current on best practices for preventing illegal robocalls. We regularly participate in fraudprevention forums and follow recommendations from regulatory bodies to improve our detection and prevention systems.

VI. Certifications

• Registration: NSG NETWORKS is registered in the FCC's Robocall Mitigation Database.

• Traceback Response: We respond to traceback requests within 24 hours.

• Compliance: NSG NETWORKS has not been subject to any regulatory or law enforcement investigation related to illegal robocall activities.

VII. Conclusion By adhering to this Robocall Mitigation Plan, NSG NETWORKS commits to actively monitoring and mitigating illegal robocall activities while maintaining compliance with regulatory standards and contributing to industry-wide anti-robocall efforts.