

Robocall Mitigation Plan - Nexusphere VOIP

Nexusphere VOIP is dedicated to maintaining the utmost standards of communication integrity and security. In line with regulatory mandates and industry norms, we have formulated a robust robocall mitigation strategy tailored to address the evolving challenges in telecommunications. Below, we detail the specific measures we have enacted to prevent the origination, transmission, or processing of illicit robocall traffic, while ensuring compliance with the know-your-upstream provider requirement as specified in section 64.1200(n)(5) of the Commission's regulations.

Regulatory Compliance: Nexusphere VOIP meticulously adheres to all pertinent laws and regulations concerning robocalls, including the Telephone Consumer Protection Act (TCPA) and the Truth in Caller ID Act, thereby upholding our legal obligations.

Advanced Robocall Detection and Prevention: Through advanced call analytics and cutting-edge machine learning algorithms, Nexusphere VOIP promptly identifies and mitigates robocalls in real-time, bolstering the resilience of our network against fraudulent activities.

Caller Identification Authentication: Our network employs sophisticated Caller Identification (ID) authentication and verification mechanisms, such as STIR/SHAKEN technology, to authenticate call origins and deter fraudulent activities effectively.

Whitelisting and Blacklisting: Nexusphere VOIP meticulously manages whitelists of trusted entities and actively maintained blacklists to proactively block known robocallers and entities suspected of engaging in suspicious activities, thereby mitigating potential threats.

Rate Limitation and Anomaly Detection: We enforce stringent rate limitation protocols on outgoing calls and leverage sophisticated anomaly detection algorithms to identify irregular call volume patterns, pivotal indicators of potential robocalling activities.

Know-Your-Upstream Provider Procedures: Nexusphere VOIP ensures rigorous compliance with the know-your-upstream provider requirement by implementing robust verification procedures to authenticate and validate the legitimacy of upstream providers engaged in call traffic.

Call Analytics Systems: Sophisticated call analytics systems are harnessed by Nexusphere VOIP to meticulously identify and mitigate illegal traffic, amplifying our capacity to mitigate the impact of robocalls on our network.

In addition to these tailored mitigation practices, we emphasize our commitment to transparency and continuous improvement:

Customer Empowerment and Education: Nexusphere VOIP empowers customers by educating them on the risks associated with robocalls and providing comprehensive guidance on configuring call settings to mitigate their impact effectively.

Collaboration and Incident Reporting: We foster collaborative partnerships with industry peers to exchange information regarding known robocallers and threats. Moreover, customers are provided with streamlined mechanisms to report suspected robocalls promptly for swift review and action.

Performance Metrics and Iterative Improvement: Nexusphere VOIP establishes a robust framework of key performance indicators (KPIs) to gauge the efficacy of our mitigation efforts. We actively solicit feedback from customers and employees to continually refine and enhance our approach.

Know Your Customer (KYC) Process - Nexusphere VOIP

Nexusphere VOIP prioritizes regulatory compliance and customer security. Our Know Your Customer (KYC) process is meticulously designed to ensure robust verification of customer identities, in strict accordance with Federal Communications Commission (FCC) guidelines, to thwart fraudulent activities and uphold the integrity of our services. Below, we outline our FCC-compliant KYC process:

Customer Identification: Upon registration or initiation of services, customers are required to furnish personal identification information, including but not limited to:

- Full legal name
- Residential address
- Date of birth
- Government-issued identification number (e.g., Social Security Number, Driver's License Number)
- Business name and address, where applicable

Document Authentication: Nexusphere VOIP employs advanced measures to authenticate the veracity of submitted documents, utilizing reputable verification services or conducting meticulous manual reviews by trained personnel.

Address Validation: For residential customers, address validation may involve cross-referencing the provided address against public records or conducting rigorous address validation checks. Business customers may be subjected to additional scrutiny, requiring

supplementary documentation such as utility bills or business licenses to validate their business address.

Risk Assessment: Nexusphere VOIP conducts a comprehensive risk assessment for each customer, considering various factors including:

- Nature of service requested
- Transaction volume
- Geographic location
- Customer's historical interactions with Nexusphere VOIP or other telecommunications providers Enhanced due diligence measures may be implemented for customers deemed to pose higher risk, necessitating additional identity verification protocols.

Continuous Monitoring: To detect and deter suspicious activities, Nexusphere VOIP implements ongoing monitoring of customer accounts and transactions, including but not limited to:

- Regular scrutiny of account activity for anomalies or high-risk transactions
- Periodic reviews and updates of customer information
- Timely response to any suspicious activity or alerts raised by our monitoring systems

Compliance Reporting: Nexusphere VOIP diligently maintains records of customer identity verification and transaction monitoring activities, as mandated by FCC regulations. We have established robust procedures for reporting suspicious activities or potential non-compliance with KYC requirements to relevant regulatory authorities.