

Robocall Mitigation Plan - Nemerald LLC

Introduction

Nemerald LLC is committed to protecting its network, customers, and the broader telecommunications ecosystem from illegal robocalls. This Robocall Mitigation Plan details the proactive measures Nemerald takes to detect, prevent, and respond to unlawful robocall traffic in compliance with the FCC's rules, including recent updates mandated by DA 24-73.

Implementation of STIR/SHAKEN

Nemerald LLC has fully implemented the STIR/SHAKEN framework across all parts of its IP-based network where technically feasible. We authenticate caller ID information for all SIP traffic and continuously monitor and update our STIR/SHAKEN deployment to ensure compliance with evolving standards and obligations.

Specific Reasonable Steps Taken to Avoid Illegal Robocall Traffic

We employ a layered approach to mitigate illegal robocalls, including the following:

- Real-time traffic analytics to detect high-volume or short-duration call patterns often associated with illegal robocalls.
- Automatic call blocking of numbers or patterns identified as high risk or previously reported for abusive behavior.
- Reputation scoring and rate limiting based on call behavior thresholds to preempt potential misuse.
- Participation in industry traceback efforts, working with the Industry Traceback Group (ITG) and law enforcement when illegal activity is detected.

Know Your Customer (KYC) Policies

To comply with our obligation to "know our customers," we have implemented strict onboarding and monitoring procedures, including:

- Manual verification of business registration and identity for each customer, including validation of EIN and corporate documentation.
- Review of intended use cases, such as call volume projections and traffic profiles, to assess risk prior to activation.
- Ongoing customer audits including monitoring of call records, complaint rates, and behavioral anomalies.
- Contractual clauses requiring customers to comply with U.S. robocall laws and granting Nemerald the right to suspend or terminate services upon detection of abuse.

Analytics Systems and Traffic Monitoring

Nemerald uses a combination of internal and external analytics tools to monitor traffic:

- Internal Systems: We maintain proprietary traffic monitoring tools that analyze call metadata in real time. These systems flag calls based on duration, frequency, destination concentration, and time-of-day patterns.
- Third-Party Analytics Vendors: We utilize services from Neustar CNAM, a leading provider of caller name identification and robocall detection services. Neustar CNAM assists in identifying high-risk or spoofed numbers, provides external scoring and call reputation insights, and enables real-time mitigation actions based on industry-wide threat intelligence.

Customer Complaints and Feedback Mechanism

Customers can report unwanted or suspicious robocalls via our dedicated hotline or web portal. Each complaint is logged and investigated by our compliance team. Findings from these investigations directly inform rule refinement and mitigation updates.

Oversight and Internal Compliance

A dedicated compliance team is responsible for implementing and overseeing this plan. This team:

- Conducts quarterly reviews of robocall mitigation procedures.
- Coordinates with network engineers and legal counsel to apply FCC guidance.
- Ensures all relevant staff receive ongoing training on robocall mitigation and STIR/SHAKEN practices.

Documentation and Regulatory Reporting

Nemerald LLC keeps detailed logs of traffic analysis, call blocking events, customer onboarding procedures, and complaint resolutions. We update our FCC Robocall Mitigation Database entry as needed and provide full cooperation during any audits or investigations.

Review and Updates to Plan

This plan is reviewed semi-annually or in response to regulatory changes, new threats, or technological developments to ensure it remains effective and compliant with 47 CFR § 64.6305 and associated public notices.