

MYKNetworks LLC - Robocall Mitigation Plan (2025)

I. Background

The Federal Communications Commission (FCC) requires all voice service providers, including MYKNetworks LLC ("MYKNetworks"), to submit certifications and Robocall Mitigation Plans to the FCC's Robocall Mitigation Database (RMD) pursuant to 47 CFR § 64.6305.

Although the Commission mandates providers to mitigate illegal robocalls, the regulations do not explicitly define the term "robocall." The TRACED Act identifies a "robocall violation" as an infringement of subsections (b) or (e) of Section 227 of the Communications Act of 1934.

Accordingly, MYKNetworks' mitigation efforts focus on preventing and addressing potential violations under these sections:

- 47 U.S.C. § 227(b): Governs calls made using prerecorded or artificial voices or an automatic telephone dialing system.
- 47 U.S.C. § 227(e): Also known as the Truth in Caller ID Act, prohibits the use of misleading caller ID information with intent to defraud or cause harm.

The FCC considers a robocall mitigation program "sufficient" if it includes well-defined practices that can reasonably be expected to reduce the origination or carriage of illegal robocalls. MYKNetworks is committed to maintaining these standards and implementing robust safeguards as outlined in this document.

II. Know Your Customer (KYC) Standards

MYKNetworks LLC performs thorough Know Your Customer (KYC) verification steps to validate each customer's legitimacy and compliance posture. The onboarding process includes completion of a KYC questionnaire, a USF Exemption Certificate (for carrier clients), and execution of a formal service agreement.

III. Acceptable Use Policy (AUP)

All MYKNetworks customers are contractually bound to comply with the company's Acceptable Use Policy (AUP). The AUP prohibits any activity involving illegal, fraudulent, or deceptive communications. MYKNetworks retains the right to suspend or terminate services for any customer violating its AUP.

IV. STIR/SHAKEN Implementation

MYKNetworks has fully implemented the STIR/SHAKEN authentication framework across its network. Customers are permitted to originate calls only from numbers assigned by MYKNetworks or from numbers for which they can demonstrate ownership.

V. Network Monitoring

MYKNetworks continuously monitors network traffic to detect suspicious or illegal robocalling activity. The company utilizes internal systems and external tools such as FraudCentral Roboguard and ZipDX's RRAPTOR for detection and blocking.

VI. Traceback Cooperation

MYKNetworks LLC is fully committed to cooperating with regulatory authorities and traceback consortiums. The company pledges to respond within 24 hours to traceback requests from the FCC, law enforcement agencies, and the Industry Traceback Group (ITG).

Date: November 2025

Prepared by: MYKNetworks LLC