

Axima Networks GmbH | Nonnendamm 33, 13627 Berlin

Federal Communications Commission
45 L Street NE
Washington, DC 20554
USA

Robocall Mitigation Plan (RMP)

rev. 4, last updated: 09/21/2025

Overview

This document provides the information required by Section 64.6305(b)(2) of FCC rules and explains the specific steps Axima Networks GmbH ("Axima") is taking to avoid originating illegal robocall traffic as part of its robocall mitigation plan (RMP) as required by Section 64.6305(a).

Axima is a Germany-based carrier, licensed to provide international voice services to wholesale and enterprise customers in compliance with the applicable laws and regulations of Germany.

Steps taken to avoid originating illegal robocalls

Axima has implemented policies, systems, and solutions to monitor, detect, and suppress any potentially fraudulent traffic (including unlawful robocalls), whether originating within its own network or transiting through it.

a. Monitoring

Axima actively monitors all traffic transiting through its network for behaviors indicative of illegal, spam, or robocalling activity:

- The presence of PAI (P-Asserted-Identity) is strictly required to pass our network
- Employs a non-intrusive CDR-based traffic pattern analysis, including
 - short duration calls and low call completion ratios
 - high volume of calls from single A-number or series
 - high volume of calls towards specific B-number

- Uses and maintains an in-house-developed control system to mitigate Call-ID spoofing. The system checks A-numbers against national dial plans and number ranges allocated by national regulators in real-time.
- The KYC (Know Your Customer) process is mandatory for all DID's sold, even in jurisdictions where end-customer registration is not currently required. The required information includes business and personal identity, addresses, and proof of address (in most EU countries).
- Maintains 24/7 NOC and point of contact for handling complaints and lawful requests.

b. Investigation and Fraud Management

Axima complies with the fraud clauses in its contracts with partners and carriers. Upon detection of suspicious traffic, Axima collaborates expeditiously and in good faith with customers, carriers, and providers to assess and determine the legitimacy of such traffic.

c. Blocking and suspending

Once fraudulent traffic (including robocalls) is detected, identified, or reported, Axima will immediately suspend the customer or carrier originating the suspicious traffic.

Traceback and Enforcement Cooperation

Axima is committed to responding fully and in a timely manner to all traceback requests from the FCC, law enforcement, the industry traceback consortium, and to cooperating with these entities in investigating and stopping illegal robocalls.

Point of contact for traceback requests: 112@aximanetworks.com