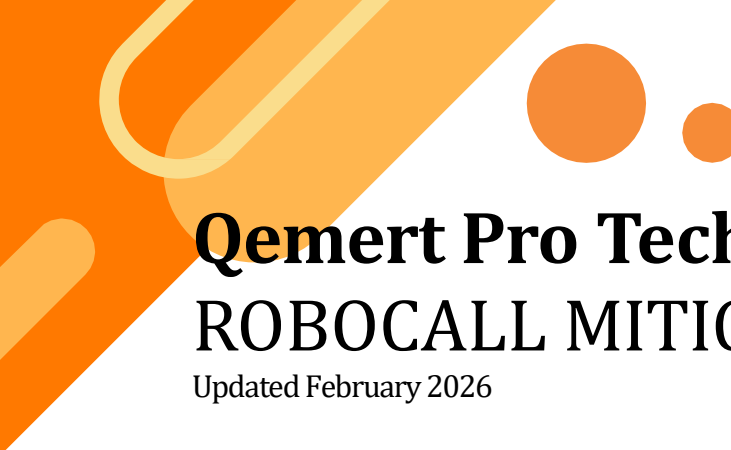




Qemert Pro Technology

ROBOCALL MITIGATION PLAN

Updated February 2026

Pursuant to 47 C.F.R. § 64.6305, Qemert Pro Technology ("Qemert") submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. This report describes the status of its implementation of STIR/SHAKEN and the practices and procedures Qemert has in place to mitigate illegal robocalls. Qemert may modify, add, delete or otherwise alter any of the policies and procedures described in the plan within ten (10) business days when filing information, services, traffic patterns, or risk controls change.

Qemert provides retail voice service to business end-user customers. Outbound calls originate from Qemert's end-user customer accounts/endpoints and route through Qemert's platform to its next-in-line carrier partner for PSTN interconnection and termination. Qemert's customers may place calls to consumers, but Qemert does not provide voice service to other voice service providers or resellers and does not accept third-party transit traffic for origination.

Qemert certifies that it has implemented STIR/SHAKEN caller ID authentication across its IP network for the calls it originates, consistent with 47 CFR § 64.630. Qemert's network is IP-based for SIP calling, and the Provider authenticates caller identification information for SIP calls it originates.

Qemert signs outbound calls it originates using its own STI certificate issued by an approved STI Certificate Authority (STI-CA) at the switch level and assigns attestation levels based on its verification of the calling party and confirmation of the calling party's authority to originate calls using the associated telephone number(s), consistent with applicable FCC rules, orders, and guidance.

Qemert is judiciously working to prevent unlawful robocalls from originating on its network and has implemented the following robocall mitigation plan to address unlawful robocall traffic.

Qemert uses affirmative measures to prevent customers from using its network to originate illegal calls, including knowing its customers and applying due diligence to deter illegal traffic.

At onboarding we collect:

- Legal business name and DBA, if applicable
- EIN and/or formation documents
- Service address
- Authorized representative
- Contact details, including email and phone
- Payment method
- Number authority/control, as applicable
- Intended use case: industry, call purpose, target geography
- Expected traffic profile: anticipated volumes and calling patterns



Customers are validated using a risk-based review, e.g., public business records where applicable, consistency checks, and whether the requested services and stated use case are reasonable, before outbound service is enabled.

Enhanced review may be triggered by unusually high projected volume, identity discrepancies, repeated caller ID changes, short-lived accounts, or indicators of lead-generation or robocall activity inconsistent with the stated use case.

Qemert has enforceable terms of use and/or an acceptable use policies noted in its contracts. These policies define the circumstances by which the company will deny, suspend, or terminate service to a customer.

Qemert has established methods and procedures to monitor its network to detect and prevent fraudulent or illegal calling activity. Qemert monitors traffic and call performance using its Ataria Systems switch, including review of call detail records and daily usage trends to identify anomalies such as unusually high volumes and bursting, short-duration spikes, abnormal ASR/ACD, high unallocated destination attempts, and caller ID irregularities (e.g., frequent changes or inconsistent presentation). When issues are identified, Qemert promptly investigates and may take corrective action, including rate-limiting, blocking, suspension, termination, and/or requesting supporting documentation, and coordinates as appropriate with upstream carrier partners and traceback requests.

Qemert does not accept third-party traffic for transit and does not receive outbound traffic from downstream resellers or other voice service providers. All inbound PSTN traffic and outbound interconnection/termination are handled through Qemert's upstream carrier partner(s) used for connectivity. Qemert maintains due diligence procedures for selecting and managing its upstream carrier partner(s), including confirming the provider relationship and points of interconnection, maintaining current contractual and contact information, and coordinating with the upstream carrier(s) on suspected illegal traffic, blocking/enforcement actions, and traceback requests as needed.

Qemert has designated an individual as a dedicated point of contact for addressing traceback requests and remains committed to responding fully and within 24 hours to call traceback requests from the Commission, law enforcement, and the traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers initiating calls.

Point of Contact:

Name: Bernardo Taveras

Title: CEO

Email: btaveras@qemert.com

Phone: 18294660410

This program demonstrates Qemert's commitment to protecting consumers, upholding industry standards, and contributing to the elimination of illegal robocalls.

