



September 23, 2025

FCC Robocall Mitigation Database Declaration

AOC Connect, LLC relies on the continuing extension from STIR-SHAKEN implementation provided under 47 CFR § 64.6304 (d) which exempts from STIR-SHAKEN Caller ID Authentication. AOC Connect does not own the network infrastructure to implement STIR-SHAKEN as it is a reseller. Therefore, AOC Connect does not have a STIR- SHAKEN implementation obligation.

Our robocall mitigation strategy remains, as it has always been:

- To refuse to service to purely outbound call centers, by enforcing clauses in our standard terms of service that require balance of the inbound/outbound traffic
- To technologically limit what CallerID numbers our customers can choose to display on outbound calls to numbers in their inventory, which we validate for ownership prior to adding
- To use automated alerting as well as manual spot checks on spikes in outbound calling patterns, to detect and stop fraudulent calls
- To assist other carriers, WITHIN 24 HOURS, in investigating any legitimate complaints of robocalling coming from numbers assigned to us, and to suspend the responsible callers if the reported calls actually originate from AOC Connect telephony providers, until the offending calling activity permanently ceases.

AOC Connect – Know Your Customer

Using internal assets, AOC Connect employs a comprehensive Know Your Customer (KYC) process to ensure that all customers utilizing our voice services are legitimate enterprises with lawful intent, and that none engage in illegal robocall or fraudulent traffic. Our KYC program is integrated into the service provisioning lifecycle and is periodically reviewed to ensure compliance with FCC rules and industry best practices.

1. Customer Identity Verification

- All prospective customers are reviewed prior to onboarding into AOC systems for service. Articles of incorporation, state registration, or business license.
- AOC Connect cross-checks business information against public databases, such as Secretary of State records, to confirm the existence and standing of the entity.

2. Traffic Use-Case Screening

- Customers are screened on service allocation for intended use cases for AOC Connect's services (e.g., enterprise communications, call centers, conferencing).
- AOC Connect prohibits service to customers engaged in:
 - o Auto-dialed mass calling campaigns without consent.
 - o Caller ID spoofing or misrepresentation.
 - o Any unlawful robocalling activity.
- Each customer's service profile is risk-assessed before activation.



3. Call Authentication & Monitoring

- All outbound calls are authenticated where technically feasible.
- Traffic patterns are continuously monitored to detect anomalies such as high-volume short-duration calls, invalid caller ID usage, or unusual call origination patterns.
- Suspect traffic triggers an immediate investigation and may result in service suspension or termination pending resolution. Investigations are monitored in AOC Connect ticketing systems.

4. Ongoing Due Diligence

- Customer records are periodically reviewed and updated to ensure continued compliance.
- Any customer flagged for non-compliant behavior is subject to an escalation process involving verification, remediation, and, if unresolved, account deactivation.
- AOC Connect cooperates fully with FCC, USAC, law enforcement, and traceback requests coordinated by the Industry Traceback Group (ITG).

Traceback and Enforcement Cooperation

AOC Connect is committed to responding within 24 hours to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG). We actively cooperate in investigations and enforcement actions to stop illegal robocallers using our network.

Certification and Updates

The Company has filed its certification and mitigation plan in the FCC's Robocall Mitigation Database. Updates to the plan and vendor disclosures will be submitted within 10 business days of any material change.

Commitment to Compliance

Through these measures, AOC Connect ensures that only legitimate and responsible customers utilize our voice network. This program demonstrates our commitment to protecting consumers, mitigating illegal robocalls, and supporting the FCC's robocall mitigation framework.

A handwritten signature in black ink that reads "Doug Thomas".

Doug Thomas
Chief Operating Officer