

Know Your Customer (KYC) Procedures – New Customers

Aethernet LLC applies a comprehensive KYC program to all new voice customers prior to enabling outbound calling. At a minimum, the Company:

Collects and verifies the customer's legal name, business entity type, tax ID (EIN), and physical business address, including documentation such as formation documents, government-issued identification for authorized signers, and proof of address.

Confirms that the customer's business purpose and proposed use case for outbound calling (e.g., call center, enterprise PBX, healthcare provider, financial institution) are legitimate and consistent with the customer's stated traffic profile.

Reviews each new customer against sanctions lists, high-risk watchlists, and performs adverse-media screening where appropriate.

Evaluates the customer's expected traffic profile, including anticipated call volumes, call durations, destinations, origination patterns, and calling windows to determine whether they align with the customer's stated use case.

Requires all customers to agree contractually not to originate illegal robocalls, to comply with the TCPA, TRACED Act, and all applicable federal/state laws, and to fully cooperate with Aethernet LLC in any investigation of suspicious or potentially unlawful traffic.

KYC Procedures – Existing Customers

Aethernet LLC applies its KYC program to existing customers as well as new ones:

The Company has conducted a retrospective KYC review of its existing customer base, prioritizing high-volume, high-risk, and atypical use cases for immediate reassessment.

Any customers failing to meet current KYC standards were required to submit updated documentation or were subject to service restrictions, enhanced monitoring, or termination, depending on risk level.

Aethernet LLC continues to periodically re-verify customer information, particularly when traffic patterns, ownership, or business operations change in a way that increases potential robocall risk.

Traffic Monitoring, Analytics, and Third-Party Vendors

Aethernet LLC continuously monitors outbound traffic for indicators of illegal robocalling. The Company uses a multi-layered analytics approach that includes:

1. Platform-Level Analytics (3CX & FreeSWITCH)

The Company utilizes analytics tools built into its 3CX and FreeSWITCH platforms, along with internal monitoring systems, to detect patterns such as:

abnormal answer/seizure ratios (ASR) extremely short-duration calls rapid-fire dialing high-risk destination patterns sequential number calling sudden, unexplained traffic spikes behavior inconsistent

with the customer's declared use case

These indicators automatically flag traffic for further review.

2. AI-Assisted Monitoring (OpenAI Models)

In addition to platform analytics, Aethernet LLC incorporates AI-enhanced analysis using OpenAI models to strengthen traffic monitoring. These tools assist with:

pattern recognition and classification
anomaly detection
clustering of suspicious calling behavior
identifying characteristics commonly correlated with illegal robocall campaigns
scoring high-risk customers and traffic segments for deeper investigation

This AI-driven layer provides enhanced intelligence and adaptability to emerging robocall tactics.

3. External Signals and Enforcement Inputs

Aethernet LLC reviews Industry Traceback Group (ITG) notices promptly.

The Company responds to all traceback requests within 24 hours and uses traceback findings to identify and remove problematic traffic.

Consumer complaints, partner notices, and law enforcement inquiries are integrated into the analytic workflow for cross-validation and escalation.

4. High-Risk Traffic Flagging and Escalation

Traffic associated with: consumer complaints, high-volume anomalies, AI-identified patterns, or traceback alerts is subject to enhanced scrutiny, including temporary blocking or immediate suspension when appropriate.

Remediation, Blocking, and Termination Procedures

When Aethernet LLC identifies suspicious, high-risk, or potentially unlawful robocall traffic:

The Company immediately initiates an investigation, contacting the customer for explanations, campaign details, and supporting documentation (such as consent records).

If the customer cannot demonstrate lawful calling activity, Aethernet LLC may: block specific call signatures or destinations, suspend outbound calling privileges, or terminate the customer's service entirely.

Aethernet LLC fully cooperates with the FCC, ITG, and any law-enforcement or regulatory body in providing call records, customer information, and mitigation actions taken, as permitted by law.

Recordkeeping and Compliance Oversight

Aethernet LLC maintains KYC records, analytics logs, monitoring results, traceback responses, and remediation actions for a sufficient retention period to support any regulatory review.

The Company has dedicated internal personnel responsible for robocall mitigation compliance, continuous monitoring, and prompt response to enforcement communications.

Conclusion

Through its comprehensive KYC program, platform-level analytics within 3CX and FreeSWITCH, AI-enhanced detection using OpenAI models, ongoing monitoring, and strict remediation and termination procedures, Aethernet LLC ensures that it does not serve as a source of illegal robocall traffic and remains in full compliance with the FCC's robocall mitigation requirements.