

ROBOCALL MITIGATION PLAN

Compliance & Certification Framework

Filer/Company Name:	Dialkore
FCC Registration Number (FRN):	0038476644
Principal Corporate Address:	700 Morse Rd, Columbus, OH 43214
Contact Email Address:	info@dialkore.com
Regulatory Authority:	Federal Communications Commission (FCC) — 47 C.F.R. § 64.6305

I. Objective and Scope

Dialkore ("the Company") is a voice service provider dedicated to preserving telecommunications infrastructure integrity, protecting consumers, and preventing the initiation or routing of fraudulent, deceptive, or illegal robocalls. This Robocall Mitigation Plan ("Plan") describes the specific, affirmative, and commercially reasonable steps implemented by Dialkore to systematically identify, avoid, and mitigate illegal robocall traffic originating from or passing through its network facility, in explicit accordance with Federal Communications Commission (FCC) mandate under 47 C.F.R. § 64.6305.

Dialkore enforces a absolute zero-tolerance standard regarding unauthorized automated outbound telemarketing, traffic pumping schemes, and deceptive caller identification (Caller ID) spoofing practices.

II. "Know Your Customer" (KYC) Onboarding Protocols

To fundamentally prevent the utilization of its service infrastructure by malicious actors or high-risk callers, Dialkore enforces comprehensive, mandated identity-vetting and "Know Your Customer" (KYC) onboarding checks prior to provisioning outbound capabilities or trunk access. These control mechanisms include:

- 1. Corporate Entity Verification:** Collecting and verifying legal business registration documents, physical address evidence, operating jurisdictions, and federally issued Employer Identification Numbers (EIN / Tax ID).
- 2. Authorized Representative Authentication:** Establishing and verifying explicit contact paths for operational management via double-authenticated corporate email domains and direct phone validation.
- 3. Traffic Profile Assessment:** Requiring commercial entities to explicitly specify their operational model, intent of traffic campaigns, expected concurrency limits, burst rates, and documentation proving their legal right-to-use any telephone numbers assigned or dynamically requested for outbound transmission.
- 4. Contractual Restrictions:** Embedding legally binding anti-robocall provisions inside Dialkore's Terms of Service (TOS) and customer agreements. The Company retains the unilateral right to immediately throttle,

isolate, or permanently disable trunk traffic without liability or notice if illegal activity or dynamic threshold parameters are broken.

III. Network Traffic Analysis & Real-Time Mitigation

Dialkore programmatically analyzes Call Detail Records (CDRs) and signaling traffic patterns across its core switching network to monitor for markers indicative of illegal robocalls or automated system abuse. Monitored signaling and operational metrics include:

- Extraordinary and sudden volume bursts from individual origin accounts over compressed temporal ranges.
- High concentrations of short-duration call events (specifically call interactions lasting under six seconds).
- Abnormally low connection and Completion-to-Attempt Ratios (CAR) indicating random/unconsented consumer sweeps.
- Sustained high volumes of parallel call distribution blocks or strict sequential dialing sets.

When system alerts flag atypical traffic, Dialkore isolates the source account and begins a manual and system audit. If the provider or downstream client fails to present reasonable verification of authentic subscriber consent or legitimate operating authority within a specified response window, Dialkore will block the specific traffic route, restrict outbound SIP operations, or terminate the client relationship to shield public network terminations.

IV. Mandatory Industry Traceback & Cooperation

Dialkore completely commits to full, direct cooperation with authorized investigative bodies seeking to mitigate illegal caller behaviors. Operational processes adhere to the following:

1. **Rapid Track Response:** Dialkore processes and fully executes traceback requests submitted via the Industry Traceback Group (ITG), the FCC, state Attorneys General, or law enforcement agencies within twenty-four (24) hours of electronic submission.
2. **Dedicated Support:** Technical engineering personnel remain assigned to trace call pathways to isolate upstream or source provider hops immediately upon verified request alerts.
3. **Immediate Upstream Enforcement:** If any client or underlying provider fails to resolve a valid robocall path issue, or if a traceback action proves structural non-compliance, Dialkore acts to sever network interconnection paths.

V. Administrative Oversight and Execution

This Robocall Mitigation Plan is maintained under executive mandate. Dialkore monitors evolving state and federal regulatory procedures to ensure technical systems match updated legal requirements.

For inquiries, operational clarifications, or formal law enforcement traceback requests regarding this corporate plan, contact the designated compliance contact point:

Authorized Network Compliance Entity: Dialkore Management

Corporate Inquiries Email: info@dialkore.com

Address of Record: 700 Morse Rd, Columbus, OH 43214