

CoreMatrix LLC operates a comprehensive robocall mitigation program designed to prevent the origination and transmission of illegal robocalls on its network, in alignment with the requirements of 47 C.F.R. § 64.6305 and related FCC rules for voice service providers. The following description is intended for use in filings with the FCC Robocall Mitigation Database and for communication with partners, customers, and regulators.

Company information

- Legal name: **CoreMatrix** LLC
- Principal address: 89 B. Karen Court, Bridgeport, CT 06606
- Website: <https://www.core-matrix.net>
- Main telephone: +1 (859) 217-4080
- Primary contact for robocall mitigation and traceback:
 - Name: Robert Harris Smith
 - Title: Chief Executive Officer
 - Email: noc@core-matrix.net
 - Phone: +1 (859) 217-4080

CoreMatrix LLC is a U.S.-based IP-enabled voice service provider interconnected with the public switched telephone network (PSTN) and the North American Numbering Plan (NANP). CoreMatrix files and maintains an active certification in the FCC Robocall Mitigation Database (RMD) and understands that U.S. intermediate and terminating providers are required to accept traffic only from entities listed in the RMD.

STIR/SHAKEN implementation status

CoreMatrix has implemented the STIR/SHAKEN call authentication framework across all feasible IP portions of its network and signs outbound calls in accordance with the FCC's caller ID authentication rules under the TRACED Act. For any legacy TDM or non-IP segments where STIR/SHAKEN cannot technically be applied, CoreMatrix subjects all unauthenticated calls to this robocall mitigation program as required by 47 C.F.R. § 64.6305(a).

CoreMatrix uses its own Service Provider Code (SPC) token and STI certificates, or qualified hosted solutions, to generate and validate SHAKEN PASSporTs and to support full attestation where customer identity, number assignment, and

call origination can be reliably verified. Calls that do not meet full attestation criteria are signed with appropriate lower attestation levels or are blocked or rejected when risk indicators are high.

Know Your Customer (KYC) and onboarding

CoreMatrix maintains strict Know Your Customer (KYC) procedures to prevent bad actors from obtaining service and using its network to originate illegal robocalls. These procedures apply to all new and existing customers, including enterprise users, wholesale VoIP customers, and any resellers:

- Customer identity verification: Collection and verification of legal business name, corporate registration, tax identification, physical address, and authorized contact information, matched against public and commercial data sources.
- Service profile review: Assessment of the customer's proposed use case (e.g., call center, alerts, two-factor authentication, enterprise PBX), anticipated call volumes, destinations, and calling patterns to ensure they are consistent with lawful purposes.
- Numbering and caller ID validation: Verification that caller IDs used by the customer are assigned by CoreMatrix or that the customer has documented authorization to use numbers from another provider, with periodic revalidation.
- Risk-based approvals: Higher-risk profiles (e.g., high-volume short-duration outbound campaigns, international origination to U.S. numbers, or prior enforcement history) are subject to enhanced due diligence, including references, additional documentation, and tighter traffic limits.

CoreMatrix reserves the right to deny service, restrict functionality, or terminate accounts where KYC cannot be satisfactorily completed or where risk cannot be adequately mitigated.

Traffic monitoring, analytics, and controls

CoreMatrix uses a combination of internal analytics and third-party tools to monitor call traffic and detect patterns indicative of illegal robocalls. This monitoring covers all outbound and transiting calls and includes:

- Real-time and retrospective analytics:

- Monitoring of calls per second (CPS), total call attempts, completion rates, and average call duration at the customer and trunk level.
- Identification of abnormal spikes in short-duration calls, high answer-but-disconnect patterns, or unusual calling to specific NPAs/NXXs.
- Reputation and numbering checks:
 - Use of “Do Not Originate” (DNO) lists, invalid or unallocated number ranges, and high-risk number databases to block or flag suspicious calling numbers at origination.
 - Integration with caller ID reputation services where feasible to identify numbers associated with abusive or fraudulent campaigns.
- Policy and routing controls:
 - Enforcement of maximum CPS, concurrent call limits, and geographic restrictions tailored to customer profiles established during KYC.
 - Blocking or rate-limiting traffic when thresholds or anomaly triggers are exceeded, pending investigation.

Traffic monitoring is reviewed by CoreMatrix’s NOC and technical leadership, including the CTO, Alex Damron, who oversees tuning of detection rules and escalation criteria.

Call blocking, mitigation actions, and enforcement

When CoreMatrix identifies traffic reasonably suspected to be illegal robocalls, it takes prompt, documented action to protect subscribers and the network, consistent with FCC guidance that robocall mitigation programs must take “specific reasonable steps” to avoid originating illegal traffic. Mitigation actions may include:

- Immediate blocking or diversion to announcements for clearly unlawful or spoofed calls (e.g., invalid caller ID, known DNO numbers, confirmed scam campaigns).
- Imposing tighter limits on affected customers, such as reduced CPS, destination restrictions, or limitations to verified caller IDs only, while investigations are conducted.

- Suspension or termination of service where CoreMatrix determines that a customer is originating or knowingly facilitating illegal robocalls, or where the customer fails to cooperate in remediation.
- Notification to upstream and downstream carriers, as appropriate, to contain large-scale or cross-network campaigns and to support industry-wide mitigation efforts.

CoreMatrix maintains written records of mitigation actions, including the basis for decisions and communications with affected customers, in order to demonstrate compliance with regulatory obligations.

Traceback cooperation and regulatory response

CoreMatrix explicitly commits to respond fully and in a timely manner to all traceback requests from the FCC, law enforcement, and the designated industry traceback consortium, as required by 47 C.F.R. § 64.6305(a)(2) and related guidance.

- Traceback handling:
 - All traceback and robocall-related inquiries received at noc@core-matrix.net are logged, acknowledged, and assigned a case owner within the NOC.
 - CoreMatrix endeavors to respond to traceback requests within 24 hours, providing call detail records and customer information to the extent permitted by applicable law and contractual obligations.
- Cooperation and follow-up:
 - Where tracebacks implicate a CoreMatrix customer, the company investigates the customer's traffic, enforces contract terms, and, where appropriate, terminates or restricts the customer's service.
 - CoreMatrix cooperates with law enforcement and regulators in efforts to identify and stop illegal robocall operations that have used its network.

Upstream, downstream, and peering practices

CoreMatrix recognizes that all providers in the U.S. call chain must maintain an active Robocall Mitigation Database filing and a documented mitigation plan. To reduce risk from interconnection partners, CoreMatrix:

- Accepts traffic only from upstream and peering partners that have current robocall mitigation or STIR/SHAKEN certifications listed in the FCC RMD, in accordance with 47 C.F.R. § 64.6305(c).
- Reviews partner and wholesale customer status in the RMD on an ongoing basis and may block or reroute traffic from entities that are not properly listed or that demonstrate non-compliant behavior.
- Incorporates robocall mitigation obligations, including cooperation with tracebacks and adherence to applicable laws, into interconnection, resale, and wholesale agreements.

Governance, training, and continuous improvement

CoreMatrix's robocall mitigation program is overseen by senior management, including the CEO, Robert Harris Smith, and the CTO, Alex Damron, who are responsible for ensuring that policies, procedures, and technical controls remain effective and aligned with evolving FCC rules and industry best practices.

- Policy management: Robocall mitigation policies are reviewed at least annually, or more frequently if the FCC updates applicable regulations or industry traceback and mitigation standards.
- Staff training: NOC personnel, customer-facing teams, and relevant technical staff receive periodic training on identifying illegal robocall patterns, handling complaints, and executing mitigation and traceback procedures.
- Program evolution: CoreMatrix monitors industry developments, including new FCC orders, enforcement actions, and best-practice resources, to refine its analytics, controls, and customer requirements over time.

Through this program, CoreMatrix LLC commits to taking reasonable, proactive steps to avoid originating illegal robocalls, to authenticate caller ID where technically feasible, and to cooperate fully with regulators and industry partners in combating unlawful robocall activity across the U.S. communications ecosystem.