

ROBOCALL MITIGATION PROGRAM DESCRIPTION

Programmatic Solutions International LLC d/b/a Digital Engines

Voice Service Provider - Initial Robocall Mitigation Database Filing

Legal Entity	Programmatic Solutions International LLC
Trade Name / DBA	Digital Engines
FCC Registration Number (FRN)	0038764122
FCC Form 499 Filer ID	839193
Primary Business Address	562 Acornridge Ln, Orange Park, FL 32065
Program Effective Date	August 17, 2026

Purpose and Commitment

Programmatic Solutions International LLC ("PSI"), operating the Digital Engines brand, maintains this Robocall Mitigation Program to prevent customers and end users from using PSI-provided voice services to originate illegal robocall traffic or unlawful caller-ID spoofing. PSI will apply this program to all calls it originates or causes to be originated through its managed voice-service environment and will update the program as its network, customer base, upstream carrier relationships, or applicable regulatory requirements change.

PSI is entering the managed/resold voice-services market and will not permit production customer traffic until the controls described in this program are in place. PSI will cooperate with the Federal Communications Commission (FCC), law enforcement, the Industry Traceback Group or other industry traceback consortium, and its upstream voice providers in investigating and stopping suspected illegal robocall traffic.

1. Service Model and Network Architecture

PSI provides managed contact-center and telecommunications-resale services to business and nonprofit customers. Services may include hosted VICIdial systems, SIP routing, DID management, outbound PSTN termination, inbound DID origination, campaign administration, and related software and infrastructure services.

Initial production architecture is expected to use customer-specific hosted dialing systems and PSI-managed OpenSIPS/SBC infrastructure, with calls delivered to approved upstream carrier(s), initially NobelBiz, for PSTN origination/termination and caller-ID authentication. PSI does not permit customers to connect arbitrary upstream carriers or present arbitrary caller-ID values without authorization.

- Customer / end-user applications: hosted VICIdial and related managed dialer systems.
- PSI voice-control layer: OpenSIPS/SBC and associated routing, logging, policy, and customer-segmentation controls.
- Upstream carrier layer: FCC-compliant originating/termination providers selected by PSI, initially NobelBiz, with backup-carrier capability planned for continuity and risk mitigation.
- Numbering: DIDs are assigned or authorized for a specific customer and campaign context. Shared, temporary, or rotation inventory is controlled by PSI and/or its upstream provider.

2. STIR/SHAKEN and Caller-ID Authentication

PSI recognizes that its RMD certification and STIR/SHAKEN obligations are separate from the commercial act of obtaining upstream termination. PSI will not represent that it independently performs STIR/SHAKEN signing unless and until it implements a compliant authentication framework applicable to its network and role.

For the initial service architecture, PSI expects qualifying calls to be authenticated by an approved upstream originating provider. NobelBiz has represented that A-level attestation may be available when the customer identity and right to use the calling number are documented. PSI will maintain the customer and DID authorization records needed to support appropriate attestation and will cooperate with its upstream provider in establishing a compliant authentication arrangement.

- PSI will prohibit use of telephone numbers that are not assigned to the customer or otherwise supported by documented authorization.
- PSI will maintain records linking customer accounts, campaigns, and authorized caller-ID numbers.
- PSI will not knowingly facilitate caller-ID spoofing intended to defraud, cause harm, or wrongfully obtain anything of value.
- If PSI changes its STIR/SHAKEN implementation status or authentication architecture, it will update its RMD filing and this program as required.

3. Know-Your-Customer and Customer Onboarding

Before enabling production voice traffic, PSI will perform risk-based customer due diligence designed to identify the actual entity using the service, the responsible individuals, the purpose of the traffic, and whether the proposed use presents heightened robocall or spoofing risk.

- Legal entity name, trade names/DBAs, physical business address, website, and business-purpose review.
- Responsible officer, technical contact, billing contact, and compliance contact information.
- Federal or state registration information reasonably appropriate to the customer type, including tax or corporate-identity information where necessary.
- Description of calling activity, including whether the customer uses predictive dialing, prerecorded messages, artificial/AI-generated voice, or other automated features.
- Expected traffic profile, including approximate volume, CPS/concurrency, geographic scope, average call duration, and calling purpose.
- Review of available adverse information or known traceback, enforcement, suspension, or illegal-robocall history where reasonably appropriate to the risk presented.
- Customer acknowledgment that it is responsible for lawful calling lists, consent where required, applicable DNC and suppression obligations, calling-hour restrictions, scripts/disclosures, recording laws, and other campaign-specific requirements.

PSI may require additional documentation or refuse, restrict, or terminate service where a customer cannot be reasonably identified, refuses to explain its traffic, presents materially inconsistent information, seeks to conceal the source or purpose of traffic, or otherwise presents unacceptable risk.

4. Telephone Number and ANI Controls

PSI will maintain controls designed to prevent unauthorized use of caller-ID numbers and to preserve traceability from an outbound call to the responsible customer and campaign.

- DID's must be assigned by PSI/upstream provider or supported by evidence of customer ownership or authorization.
- ANI/DID rotation, local-presence selection, and campaign pools may be used for legitimate business purposes, but rotation does not authorize spoofing or obscure customer accountability.
- PSI will retain sufficient routing/CDR information to identify the customer, campaign, displayed caller ID, destination, timestamp, and relevant call disposition for traceback and investigation purposes.
- Numbers identified as compromised, misused, improperly assigned, or associated with suspicious traffic may be quarantined, removed from outbound use, or released as appropriate.

5. Campaign Compliance and Suppression Controls

PSI provides technology controls to support lawful calling, but customers remain responsible for determining whether a specific call is legally permitted. PSI will maintain customer- and campaign-specific controls capable of enforcing suppression and dialing restrictions supplied or configured for the customer.

- Customer-specific and campaign-specific do-not-call/suppression lists.
- National Do Not Call Registry screening where applicable to the customer and campaign and where PSI is authorized to perform such screening.
- Additional state or customer-specific suppression sources where supported and contractually enabled.
- Campaign isolation so that a compliance or reputation issue can be contained to the affected customer, campaign, or DID pool where practicable.
- Reasonable dialing-policy controls, including calling-hour, retry, and campaign configuration controls where configured for the customer.

6. Prerecorded and Artificial/AI-Generated Voice

PSI expects its primary service mode to be attended, live-agent calling. PSI may support attended artificial/AI-generated voice or human-triggered prerecorded audio only when explicitly enabled for a customer or campaign. PSI will treat delivery of prerecorded or artificial/AI-generated voice as a heightened-risk feature requiring separate review of the proposed use and applicable customer compliance obligations.

- AI used solely to suggest text to a live agent is treated separately from AI-generated voice delivered to the called party.
- Attended AI voice or human-triggered prerecorded playback does not bypass applicable artificial/prerecorded voice rules.
- Fully unattended automated AI voice calling is not PSI's default service mode and will not be enabled without separate technical, contractual, and compliance review.

7. Traffic Monitoring and Detection

PSI will monitor available operational information for patterns that may indicate illegal robocalling, spoofing, fraud, or material deviation from the customer profile established during onboarding. Monitoring will be risk-based and may use automated thresholds, carrier feedback, customer complaints, CDR analysis, and manual review.

- Unusual or unexplained spikes in volume, CPS, destinations, or short-duration calls.

- Material deviations from the customer's stated calling purpose or expected traffic profile.
- Repeated carrier complaints, traceback requests, blocking notices, fraud alerts, or caller-ID reputation issues.
- Use of unauthorized or unexplained caller-ID numbers.
- Patterns suggesting attempts to evade suspension, customer identification, or number-level enforcement.

8. Response to Suspected Illegal Traffic

When PSI identifies or receives credible notice of suspected illegal robocall traffic, PSI will take reasonable, proportionate action based on the facts available and the urgency of the risk. Where practicable, PSI will contain the affected traffic without unnecessarily disrupting unrelated lawful traffic.

Possible actions include: temporary campaign suspension; DID or ANI quarantine; reduced CPS or concurrency; blocking a destination or calling pattern; requiring additional customer documentation; disabling prerecorded/AI functions; escalation to an upstream carrier; or full customer suspension/termination where warranted.

PSI may act immediately without advance notice when necessary to respond to an active traceback, carrier or regulatory directive, material fraud/security risk, suspected illegal spoofing, or other circumstances where delay would materially increase the risk of illegal traffic or harm.

9. Traceback and Regulatory Cooperation

PSI commits to respond fully and within 24 hours to traceback requests from the FCC, law enforcement, and the industry traceback consortium, consistent with applicable FCC rules. PSI will maintain a monitored compliance contact and procedures intended to identify the responsible customer and relevant call records promptly.

- Traceback requests are treated as priority compliance incidents.
- PSI will preserve and provide reasonably available call-routing and customer-identification information needed to identify the source of traffic.
- Customers are contractually required to cooperate promptly with PSI requests for information needed for traceback, regulatory, carrier, or law-enforcement inquiries.
- PSI will cooperate with upstream providers in blocking or mitigating confirmed or credibly suspected illegal traffic.

10. Recordkeeping

PSI will maintain records reasonably sufficient to support customer identification, caller-ID authorization, billing, traceback response, and enforcement of this mitigation program. The precise retention period may vary by record type, contract, and legal requirement; PSI will maintain core customer identity and telecommunications records for a period reasonably adequate to support regulatory and traceback obligations.

- Customer onboarding/KYC records and responsible contacts.
- Authorized DID/ANI assignments and supporting authorization information.
- Relevant CDRs and routing records.
- Campaign and suppression configuration records where maintained by PSI.

- Material compliance notices, traceback requests, investigation records, and resulting remedial actions.

11. Upstream Provider and Supply-Chain Controls

PSI will use commercially reasonable diligence when selecting upstream voice providers and will seek to use providers that maintain required FCC registrations and RMD certifications applicable to their role. PSI will not knowingly route U.S. voice traffic through a provider that PSI knows is prohibited from carrying or receiving such traffic under applicable FCC rules.

PSI plans to maintain backup-carrier and migration capability to reduce dependency on any single upstream network. Business-continuity measures do not replace robocall-mitigation obligations; any backup carrier used for production traffic will be subject to the same customer-identification, caller-ID authorization, traceback, and regulatory controls described in this program.

12. Internal Responsibility, Training, and Governance

PSI designates a responsible officer/compliance contact to oversee this program, manage RMD and upstream-carrier compliance matters, coordinate traceback responses, and approve material changes to voice-service risk controls.

- Personnel with administrative access to voice-routing or caller-ID systems will be instructed not to bypass customer-identity or ANI authorization controls.
- Material compliance incidents will be escalated to PSI ownership/management.
- PSI will periodically review whether its controls remain appropriate as services expand, including any future wholesale activity, expanded AI functionality, or changes in STIR/SHAKEN architecture.

13. Program Review and RMD Updates

PSI will review this Robocall Mitigation Program periodically and when there is a material change in its voice-service architecture, customer risk profile, authentication arrangements, upstream carrier relationships, or applicable FCC requirements. PSI will update its RMD filing within the time required by FCC rules when information in the filing materially changes and will complete required annual RMD recertification.

14. Regulatory Basis

This program is designed to support PSI's obligations as a voice service provider under the FCC's caller-ID authentication and robocall-mitigation rules, including 47 C.F.R. Part 64, Subpart HH, and particularly 47 C.F.R. § 64.6305. PSI will interpret and update the program in light of applicable FCC orders, public notices, enforcement guidance, and amendments to the governing rules.

Program Approval

This document describes the robocall-mitigation practices that Programmatic Solutions International LLC intends to have in effect before permitting production customer voice traffic and to maintain thereafter. PSI will not knowingly permit its services to be used to originate illegal robocalls or unlawful caller-ID spoofing and will take reasonable measures to investigate and stop such activity when identified.

Responsible Officer: Jonathan Will

Title: Owner / Managing Member

Effective Date: August 17, 2026

FCC FRN: 0038764122 | FCC Form 499 Filer ID: 839193

Reference Notes

- 47 C.F.R. § 64.6305 - Robocall mitigation and certification.
- FCC Robocall Mitigation Database External Filing Instructions (current filing instructions).
- FCC Public Notice DA 24-73 - revised Robocall Mitigation Database filing requirements.
- FCC Enforcement Advisory DA 26-174 - RMD and traceback compliance obligations.