

PARAMOUNT ENERGY SOLUTIONS INC. d/b/a DIALCS COMMUNICATIONS

Robocall Mitigation Plan

For submission to the FCC Robocall Mitigation Database

Legal filing entity	Paramount Energy Solutions Inc.
DBA / trade name	DIALCS Communications
Provider capacity	Voice Service Provider
Regulatory identifiers	OCN 208L FCC Form 499 Filer ID 837523 FRN 0036811537 RMD0027438
Compliance contact	Sam Khan Sam@dialcs.com +1 (825) 904-6638
Plan version	Version 1.1 August 9, 2026

OFFICER VERIFICATION REQUIRED Before filing, DialCS must insert the names of any third-party analytics or upstream providers relied upon and confirm that Option 1 is accurate under the FCC test described in Section 3. Do not file a statement that does not match actual operations.

This plan describes the affirmative and effective measures used by Paramount Energy Solutions Inc., doing business as DIALCS Communications ("DialCS"), to prevent its network and services from being used to originate illegal robocalls or transmit unlawfully spoofed traffic. It is designed to satisfy 47 C.F.R. §§ 64.6305(a) and 64.6305(d)(2)(ii), including DialCS’s customer due-diligence, upstream-provider review, call analytics, traceback, investigation, blocking, and remediation practices.

1. Company and Service Profile

Paramount Energy Solutions Inc., doing business as DIALCS Communications, is a United States voice service provider registered under FRN 0036811537, FCC Form 499 Filer ID 837523, OCN 208L, and Robocall Mitigation Database ID RMD0027438. DialCS offers IP-based voice services to business end users. Its services may include SIP trunking, outbound and inbound voice connectivity, local and toll-free number services, and related call-routing functionality. DialCS does not knowingly permit any customer to use its services for unlawful spoofing, fraudulent impersonation, illegal prerecorded or artificial-voice calls, or calls made without legally required consent.

This plan applies to every call originated by a DialCS end user and to all personnel, systems, contractors, vendors, and upstream carriers involved in provisioning or carrying that traffic. DialCS treats robocall mitigation as a condition of customer onboarding and continued service—not merely as a response after a complaint.

2. Governance and Accountability

The company officer responsible for this filing has ultimate accountability for this program. The designated robocall mitigation contact coordinates compliance, network operations, customer onboarding, complaint handling, traceback responses, suspensions, terminations, and required RMD updates.

- Robocall mitigation and compliance contact: Sam Khan, Sam@dialcs.com, +1 (825) 904-6638. The company must ensure his title and business address are also complete and current in the RMD portal.
- Traceback requests are treated as urgent compliance incidents and escalated immediately to management and network operations.
- DialCS maintains written records sufficient to identify the customer, source IP or trunk, calling and called numbers, timestamps, upstream/downstream route, STIR/SHAKEN result, and action taken.
- Personnel with provisioning or routing access are trained to escalate suspicious traffic and must not override compliance blocks without documented authorization.

3. STIR/SHAKEN Caller-ID Authentication

DialCS will select “Option 1 – Complete STIR/SHAKEN Implementation” only if its entire network is IP-based, it is registered with the STI Policy Administrator, it possesses its own Service Provider Code token and a valid Secure Telephone Identity certificate, and every call it originates is authenticated using that certificate, directly or through a third party. If a third party performs the technological signing function, DialCS must still make the attestation decision and all calls must be signed with DialCS’s certificate, not the third party’s certificate.

DO NOT FILE OPTION 1 UNLESS CONFIRMED Confirm in writing: (1) active STI-PA registration; (2) DialCS SPC token; (3) valid DialCS certificate; (4) all originated calls signed;

and (5) no non-IP portion of the network. Otherwise, select the legally correct option and state the applicable exemption or extension.

DialCS assigns attestation based on verified customer identity and authorization to use the calling number:

- A-level attestation only when DialCS has authenticated the customer and verified the customer's right to use the displayed calling number.
- B-level attestation when the customer is authenticated but DialCS cannot verify the customer's right to use the displayed number.
- C-level attestation only where DialCS has no direct relationship with the originator and is acting in a role for which that attestation is technically and legally appropriate.

DialCS does not upgrade attestation merely to improve call completion. It monitors signing failures, certificate validity, Identity-header errors, inconsistent attestation, and unsigned traffic. Material failures are investigated promptly and affected routing may be restricted until corrected.

4. Know-Your-Customer Program

Before activating service, DialCS obtains and evaluates information sufficient to establish the customer's identity, legitimacy, intended use, and calling-number authority. Review is risk-based and is repeated when information changes or risk indicators arise.

Minimum onboarding controls include:

- Legal business name, physical address, jurisdiction and formation records; EIN or equivalent tax identifier where applicable; website and business-domain email; and responsible principal/contact information.
- Government-issued identification for an authorized representative when appropriate, together with verification that the representative may bind the customer.
- Description of the customer's business, call purpose, expected recipients, anticipated volume, calling hours, geographic patterns, average call duration, and use of prerecorded or artificial voice.
- Evidence of the right to use each outbound calling number, including number assignment, porting, or letter-of-authorization records. DialCS prohibits arbitrary user-supplied caller ID.
- For telemarketing or lead-generation use cases, documentation addressing consent, Do-Not-Call compliance, campaign scripts, opt-out handling, lead source, and vendor/subcontractor relationships.
- Sanctions, adverse-media, regulatory, fraud, and internal-history review appropriate to the customer's risk profile.

DialCS rejects or escalates applications involving unverifiable identities, nominee or shell arrangements, unexplained use of residential or virtual addresses, disposable contact information, mismatched domains, high-risk impersonation themes, spoofing requests,

misleading scripts, implausible traffic forecasts, prior carrier terminations, or resistance to compliance questions.

5. Customer Risk Classification and Enhanced Due Diligence

DialCS classifies customers as standard, elevated, or prohibited risk. Elevated-risk customers—including high-volume outbound callers, lead generators, telemarketers, debt collectors, healthcare or financial campaigns, short-duration traffic, or customers using many calling numbers—receive enhanced due diligence, tighter initial limits, closer monitoring, and periodic re-verification.

DialCS does not activate prohibited use cases. Where risk can be controlled, DialCS may impose a probationary period, limited channels or calls per second, verified-number allowlists, destination restrictions, daily volume caps, additional deposits, or pre-approval of campaigns. Limits are increased only after traffic demonstrates a legitimate and stable pattern.

6. Know-Your-Upstream-Provider Procedures

Before accepting service from an upstream or interconnecting provider, DialCS verifies the provider's legal identity, contact details, role in the call chain, relevant authorization, and current RMD status. DialCS performs periodic and event-driven rechecks and will not knowingly accept traffic directly from a provider whose RMD filing is absent or has been removed where FCC rules prohibit acceptance.

- DialCS documents interconnection points, authorized IP addresses, trunk identifiers, escalation contacts, and contractual allocation of STIR/SHAKEN and traceback responsibilities.
- DialCS requires prompt cooperation with traceback and fraud investigations and the ability to block or isolate suspicious traffic.
- DialCS investigates unexplained changes in routing, caller-ID treatment, attestation, call completion, or complaint patterns and may reroute, suspend, or terminate the relationship.

7. Call Analytics and Network Controls

DialCS uses internal network and account-level monitoring to identify traffic inconsistent with a customer's verified profile. The company evaluates multiple indicators in context and does not rely on a single threshold to determine illegality.

- Sudden spikes in attempts, calls per second, concurrent calls, destinations, or number rotation;
- High proportions of very short calls, repeated calls to the same recipients, abnormal answer/seizure patterns, or traffic outside the approved schedule;
- Invalid, malformed, unassigned, unallocated, disconnected, or unauthorized caller-ID numbers;

- Caller-ID names or scripts suggesting government, financial-institution, healthcare, utility, carrier-support, or other impersonation;
- STIR/SHAKEN failures, unsigned IP traffic, attestation inconsistent with customer verification, certificate or Identity-header errors, and repeated downstream treatment as spam;
- Consumer complaints, traceback appearances, honeypot indicators, upstream/downstream carrier alerts, and reputation-labeling reports;
- Traffic materially inconsistent with the customer's disclosed business, campaign, recipient base, expected volume, geography, duration, or call purpose.

Controls may include automated rejection, rate limiting, verified-caller-ID allowlists, destination or prefix blocking, CPS/channel restrictions, account quarantine, manual review, temporary suspension, and permanent termination. DialCS applies safeguards intended to avoid blocking emergency calls and takes care regarding public-safety calling patterns.

DISCLOSURE TO COMPLETE If DialCS relies on a third-party analytics vendor or an upstream carrier's analytics, insert the provider name(s) here before filing: [INSERT ANALYTICS VENDOR / UPSTREAM PROVIDER NAME(S)]. If none are used, state: "DialCS does not use a third-party analytics vendor and performs the measures described above internally."

8. Ongoing Monitoring and Periodic Review

Monitoring begins at activation and continues throughout the customer relationship. DialCS compares actual traffic with the verified profile, reviews alerts and complaints, and conducts periodic re-verification proportionate to risk. Customer identity, ownership, contact details, business purpose, number authority, campaign information, and expected traffic must be refreshed when they change and at intervals appropriate to risk.

Triggers for immediate review include a traceback, law-enforcement request, credible complaint, carrier fraud notice, sharp traffic change, unauthorized caller ID, failed payment combined with risk indicators, adverse regulatory information, or evidence that a customer supplied false or incomplete information.

9. Complaints, Tracebacks, and Investigations

DialCS commits to respond fully and within 24 hours to every traceback request from the FCC, law enforcement, and the registered industry traceback consortium, and to cooperate in investigating and stopping illegal robocallers using its service.

Upon receiving a traceback or credible illegal-traffic report, DialCS will:

1. Acknowledge and triage the request immediately; preserve relevant call-detail records, SIP signaling, account records, routing information, and customer communications.

2. Identify the originating customer, source trunk or IP, calling number, downstream route, and relevant upstream provider; provide responsive information through the authorized channel.
3. Contain the risk through blocking, rate limiting, trunk isolation, suspension, or termination when facts warrant, without waiting for a pattern to continue.
4. Require the customer to provide a prompt, documented explanation and proof of lawful calling authority; reject unsupported explanations.
5. Notify and coordinate with affected upstream or downstream providers and government or traceback personnel as appropriate.
6. Document the cause, scope, corrective action, decision maker, completion time, and any changes needed to controls or customer risk classification.

10. Blocking, Suspension, and Termination

DialCS may block individual calls, calling numbers, destinations, trunks, IP addresses, or entire accounts when traffic is illegal, unauthorized, deceptive, suspicious, inconsistent with the approved use case, or presents an unacceptable risk. DialCS may act immediately when delay could permit consumer harm.

Grounds for suspension or termination include illegal spoofing, fraudulent impersonation, failure to honor opt-out or Do-Not-Call obligations, inability to prove consent where required, unauthorized number use, evasion of traffic controls, submission of false KYC information, refusal to cooperate, repeated traceback appearances, material contract breach, or any use likely to expose DialCS or the public to harm.

A terminated customer may not reactivate through an affiliate, new account, alternate identity, reseller, or other evasion method. DialCS records the termination and screens future applications for related principals, domains, addresses, payment methods, IP addresses, and calling patterns.

11. Contractual Robocall-Mitigation Controls

DialCS's customer agreements, acceptable-use terms, or service orders prohibit illegal robocalls, unlawful spoofing, fraud, misleading caller ID, unauthorized use of numbers, and violation of the TCPA, Truth in Caller ID Act, Telemarketing Sales Rule, Do-Not-Call requirements, and other applicable law. They require customers to:

- Use services only for lawful, disclosed purposes and obtain all required consent;
- Maintain accurate KYC, campaign, number-authorization, and contact information;
- Honor opt-out and Do-Not-Call requests and maintain required suppression procedures;
- Provide records, scripts, consent evidence, and explanations promptly when requested;
- Cooperate with DialCS, carriers, the FCC, law enforcement, and the traceback consortium;
- Accept DialCS's right to monitor, restrict, block, suspend, or terminate service without advance notice when needed to prevent unlawful or harmful traffic;

- Not resell, sublicense, or provide access to third parties unless expressly approved and subject to equivalent compliance obligations.

Agreements with upstream providers require appropriate robocall-mitigation, STIR/SHAKEN, routing-integrity, complaint, and traceback cooperation. DialCS does not treat contractual promises as a substitute for operational monitoring and enforcement.

12. Record Retention and Audit Trail

DialCS retains KYC and number-authorization records, service agreements, material campaign records, relevant call-detail records, traceback and complaint correspondence, investigation notes, suspension and termination decisions, and control changes for a period reasonably sufficient to support compliance, contractual, litigation-hold, and law-enforcement needs, and for any longer period required by applicable law. Access is limited to personnel with a business need, and records are preserved when an investigation or legal hold applies.

13. Program Testing, Review, and Improvement

DialCS reviews this program at least annually and after material incidents, regulatory changes, new products, significant traffic changes, or control failures. Reviews evaluate whether onboarding controls, attestation practices, analytics, thresholds, escalation paths, contractual terms, staff training, and response times remain effective. Identified gaps are assigned to an owner and tracked through remediation.

DialCS will update its RMD filing within 10 business days when information required by the FCC changes and will complete annual recertification on or before March 1. The responsible officer will verify that the public filing accurately reflects current operations before signing.

14. Certification Commitments

Subject to officer verification of the facts stated in this plan, DialCS certifies and commits that:

- All calls originated on its network are subject to this robocall mitigation program;
- It takes reasonable, affirmative, and effective steps to avoid originating illegal robocall traffic;
- It will respond fully and within 24 hours to traceback requests from the FCC, law enforcement, and the industry traceback consortium;
- It will cooperate in investigating and stopping illegal robocallers that use its service;
- It will enforce this plan in practice and will not knowingly permit customers to evade its controls;
- Its RMD filing and supporting statements will be accurate, complete, and kept current.

15. Officer Pre-Filing Verification (Internal Checklist)

REMOVE OR COMPLETE BEFORE PUBLIC FILING This checklist is included to prevent an inaccurate certification. Complete every item, replace the analytics disclosure in Section 7, then the officer may retain or remove this section from the public filing copy.

- ☐ Exact legal name is Paramount Energy Solutions Inc., with DIALCS Communications disclosed as its DBA/trade name, and both match CORES/FRN records.
- ☐ OCN 208L, FCC Form 499 Filer ID 837523, FRN 0036811537, and RMD ID RMD0027438 are correct and belong to the filing entity.
- ☐ Provider role selected in the portal accurately describes DialCS's actual role(s).
- ☐ The prior-two-year regulatory-action answer covers DialCS and all entities sharing ownership, management, directors, or control.
- ☐ DialCS's entire network is IP-based.
- ☐ DialCS has active STI-PA registration, its own SPC token, and a valid STI certificate.
- ☐ Every originated call is authenticated using DialCS's certificate; DialCS makes attestation decisions.
- ☐ The analytics disclosure names every third party or upstream provider relied upon, or expressly states none.
- ☐ The KYC, monitoring, blocking, traceback, contract, and record practices described here are implemented—not merely planned.
- ☐ The officer has reviewed the final PDF and can sign under 47 C.F.R. § 1.16.

16. Signature

The undersigned acknowledges this Robocall Mitigation Plan on behalf of Paramount Energy Solutions Inc. d/b/a DIALCS Communications and confirms that the information stated herein is accurate to the best of the undersigned's knowledge as of the date below.

Electronic signature	/s/ Sam Khan
Printed name	Sam Khan
Capacity	Compliance Contact
Date	August 9, 2026

Sources and Regulatory Basis

47 C.F.R. § 64.6305(a), (d) and (h), Robocall mitigation and certification.

47 C.F.R. § 64.1200(n), including customer and upstream-provider due diligence and traceback obligations.

FCC, Robocall Mitigation Database Frequently Asked Questions for Filers, updated January 20, 2026.

FCC, Robocall Mitigation Database External Filing Instructions.

TRACED Act, Pub. L. No. 116-105, and the Truth in Caller ID Act, 47 U.S.C. § 227(e).

This operational compliance plan is not a legal opinion. DialCS should have an authorized officer and, where appropriate, U.S. telecommunications counsel confirm that the final filing matches actual operations and all current FCC requirements.