

Robocall Mitigation Program Description

PEAK MARKETING GROUP, INC.

Effective / last updated: September 28, 2026

Field	Value
Legal entity	PEAK MARKETING GROUP, INC.
EIN	32-0867991
FCC business FRN	0038934568
FCC Form 499 Filer ID	839322
OCN / Company Code	Not assigned
RMD ID	Not assigned
DBA / assumed name (telecom)	None
Principal / mailing address	6701 Corporate Dr STE 4653, Johnston, IA 50131
Public telephone	888-488-9069
Public email	contact@peakmarketgrp.com
Traceback / mitigation email	compliance@peakmarketgrp.com
Website	https://peakmarketgrp.com
Program owner / certifying officer	Rustphine Lalas, President
Mitigation contact	Rustphine Lalas, President · compliance@peakmarketgrp.com · 317-303-4337
Foreign voice provider	No
STIR/SHAKEN implementation	Not implemented on any portion of the network (pending)
Live customer voice traffic	None meaningful as of this description — do not claim live traffic
Upstream platform (ops note)	To be confirmed for Peak entity — no Account SID listed in this filing

1. Scope and objective

Peak Marketing Group, Inc. ("Peak") maintains this robocall mitigation program to prevent its services, telephone numbers, personnel, contractors, customers, and any downstream users of Peak-provided voice access from originating, carrying, or transmitting illegal robocalls or calls with unlawfully spoofed caller identification.

Peak is a U.S. IP-enabled (IPES) interconnected VoIP and business communications provider offering managed SIP voice and related business communications for **approved business customers**.

Service description: Peak Marketing Group, Inc. provides U.S. business communications and managed interconnected VoIP services for approved business customers. Services include inbound and outbound SIP voice, DIDs and toll-free numbers, call routing and failover, Caller ID management consistent with lawful identity, live-agent sales follow-up, lead qualification, customer service, alerts, and related call-handling support. Traffic is limited to verified business use cases; purchased-list messaging and use of consent captured for another sender are not accepted. Robocall mitigation, STIR/SHAKEN authentication (as implemented), traceback cooperation, and complaint/opt-out handling are part of the operating controls.

This program applies to every call Peak originates or transmits and to every account, campaign, number, route, and user with access to Peak-provided voice services. Until STIR/SHAKEN is actually implemented for Peak (see Section 8), **all** traffic remains subject to the non-STIR controls in this program. The presence or absence of an Identity header is not a substitute for customer verification, lawful-basis review, traffic monitoring, complaint handling, or traceback cooperation.

Peak does **not** claim complete or partial STIR/SHAKEN implementation in this filing.

Peak does **not** claim live customer voice traffic in this filing.

2. Provider role and network posture

As of this description:

- Peak intends to operate as a **domestic voice service provider with a STIR/SHAKEN implementation obligation serving end-users**, offering IP-enabled (IPES) interconnected VoIP to approved business customers.
- Peak is **not** a gateway provider.
- Peak does **not** hold an OCN, STI-PA account, SPC token, or STI-CA certificate in its own name.
- Peak has **not** implemented STIR/SHAKEN on any portion of its network.
- Peak is **not** originating or carrying meaningful live customer voice traffic.
- Geographic orientation: United States. Principal operations identity is Johnston, Iowa. Jurisdictions served will match Peak's FCC Form 499-A certifications.
- First expected U.S. interconnected VoIP operations period: **October 2026**.

Peak will not reuse another legal entity's identifiers, certificate, filings, brand, or consent evidence.

Peak lists **no DBA** on this RMD.

3. Governance and accountability

- The **President**, Rustphine Lalas, owns this program, approves material changes, and has authority to refuse onboarding, suspend traffic, accounts, campaigns, numbers, vendors, or routes, and to terminate access.
- The mitigation / traceback contact (compliance@peakmarketgrp.com / 317-303-4337) monitors regulatory, complaint, and traceback communications and coordinates responses, record preservation, remediation, and carrier communications. Public contact remains contact@peakmarketgrp.com / 888-488-9069.
- Personnel and contractors with calling or network access must follow this program and may use only approved accounts, numbers, platforms, routes, data sources, and call purposes.
- Peak reviews this program after a material incident or regulatory change and at least annually, recertifies in the Robocall Mitigation Database by **March 1** each year, and updates the RMD filing within **10 business days** of a material change (including STIR/SHAKEN implementation status, contact information, ownership, or named vendors).

This description does not limit additional operational, contractual, or legal controls that may apply.

4. Know-your-customer (KYC) for voice customers

Peak does not grant unmanaged, anonymous, or "pay-and-dial" voice access. Before activating or materially expanding voice access for a customer, Peak requires information sufficient to understand **who** will use the service, **what** traffic will be sent, and whether that use is lawful. Review is proportionate to risk and includes, as applicable:

Identity and business verification

- Legal name, physical address, responsible individual, working telephone and email, and business-formation or comparable identity documentation.
- Confirmation that the customer is a business (not an unidentified consumer originator) and that the named authorized user is associated with that business.

Authorized-user and number-authorization checks

- Identification of persons authorized to place or administer calls.
- Evidence of authority to use each calling number (Peak-assigned DID/toll-free, or customer-provided numbers with documented authorization).
- Prohibition on supplying false, misleading, randomly generated, or unauthorized caller identification.

Intended-use and traffic-profile review

- Nature of the business, intended calling use case, expected volumes, calling hours, geographic footprint, and the relationship among the caller, the called party, and any represented seller.
- Confirmation that the use case is a **verified business** purpose consistent with Section 5.
- Expected consent or other lawful basis when outbound campaigns require consent.

High-risk indicators and enhanced review

Additional review, delayed activation, limits, or rejection when information is incomplete, inconsistent, unverifiable, associated with prior complaints or traceback, appears to involve purchased lists or recycled consent, or otherwise presents elevated robocall risk.

Ongoing monitoring and re-verification

- Material changes in use case, volume, calling numbers, or ownership trigger re-review.
- Complaint concentrations, carrier warnings, or traceback activity trigger enhanced review of the implicated customer.

Suspension and termination

Peak may throttle, block, suspend, or terminate a customer, campaign, number, or route immediately when KYC cannot be substantiated, when illegal or abusive traffic is indicated, or when the customer refuses timely cooperation with traceback or complaint investigation.

5. Permitted traffic; no purchased-list messaging

Traffic on Peak voice services is limited to **verified business use cases** for approved customers.

Accepted (subject to KYC and use-case approval): inbound and outbound SIP voice; DID's and toll-free; call routing and failover; Caller ID management consistent with lawful identity; live-agent sales follow-up; lead qualification; customer service; alerts; and related call-handling support.

Not accepted:

- Purchased, rented, scraped, aged, shared, or affiliate lead lists used as a consent source or as a substitute for sender-specific consent.
- Use of consent captured for **another sender**.
- Unlawful prerecorded or artificial-voice calls, unlawful autodialed calls, caller-ID spoofing, impersonation, fraud, or evasion of carrier or regulatory controls.
- Unmanaged "list blast" voice programs.

Third-party lead or consent certificates, if ever presented, are supporting evidence only — not conclusive proof. Peak may validate the source, disclosure language, seller identity, consumer data, IP and timestamp information, and whether a number may have been reassigned. A source or campaign is suspended when consent cannot be substantiated or credible contrary evidence arises.

6. Do-not-call, suppression, and opt-out

- Campaign operators and Peak-operated live-agent programs must maintain records supporting the lawful basis for calls and must honor **company-specific do-not-call** requests and applicable federal and state DNC / suppression rules.
- Consumers and called parties may request no-further-contact through published channels: contact@peakmarketgrp.com, compliance@peakmarketgrp.com, and 888-488-9069. Such requests are recorded and applied to Peak-controlled calling.
- Peak does not currently name a third-party DNC-scrub vendor in this plan. If a vendor is later used, this plan and the RMD filing will be updated within 10 business days to identify it.

7. Analytics, monitoring, and complaint handling

Analytics / monitoring (no invented vendors). Peak does **not** currently use a named third-party robocall analytics vendor. Traffic and abuse review is performed operationally by the President and designated operations personnel using information reasonably available to Peak, including:

- customer identity and approved use case;
- calling and called numbers, date/time, and available call-detail or platform logs;
- sudden volume changes, unusually high short-duration or unanswered-call rates, repeated calls to the same destinations, invalid or unassigned calling numbers, and inconsistent patterns versus the approved profile;
- complaint concentrations;
- carrier or downstream-provider warnings; and
- traceback or law-enforcement notices.

Traffic or a campaign presenting elevated risk is subject to investigation, additional documentation requirements, throttling, temporary blocking, number or route restrictions, or suspension.

If Peak later engages a third-party analytics vendor, Peak will name that vendor in an updated plan and RMD filing within 10 business days and will not imply vendor coverage that does not exist.

Complaint handling. Complaints received at contact@peakmarketgrp.com, compliance@peakmarketgrp.com, or 888-488-9069 (or referred by a carrier, the FCC, or a state agency) are logged, tied to the relevant customer/campaign/number where identifiable, investigated, and answered. Credible complaints can result in immediate traffic restriction pending investigation.

8. STIR/SHAKEN status — pending implementation (not complete)

Certification selection for the RMD portal: Peak has **not implemented** the STIR/SHAKEN authentication framework on **any** portion of its network.

Truthful current facts:

- Peak's STIR/SHAKEN work is **pending implementation**.
- Peak does not hold a Peak-specific OCN, STI-PA enrollment, SPC token, or STI-CA certificate.
- Peak has not deployed a Peak signing platform (STI-AS/VS) and does not sign calls in Peak's own name.
- Peak will not certify complete or partial implementation merely because an application is in progress, because another entity has implemented STIR/SHAKEN, or because a vendor account exists.

Intended path (not a claim of completion): FCC business FRN → USAC Form 499-A → this RMD filing → NECA Company Code/OCN when interconnection and customer proof exist → STI-PA enrollment → SPC token → approved STI-CA certificate → deploy signing for applicable IP-originated calls at the highest attestation supported by verified caller identity and numbering authority.

Until that path is complete for **this** legal entity, all traffic remains subject to the KYC, use-case, DNC, monitoring, complaint, and traceback controls in this program.

When Peak can truthfully certify a change in implementation status, it will update the RMD within 10 business days.

Peak does not, in this filing, claim a Commission implementation **extension** under 47 CFR § 64.6304. Non-implementation at this stage reflects that required identifiers and signing credentials have not yet been obtained for this entity. Peak is diligently pursuing implementation.

9. Upstream and downstream provider controls

Before Peak accepts voice traffic from, or sends voice traffic to, another provider in a Peak-controlled arrangement, Peak will:

- confirm the counterparty's legal identity and, where applicable, presence in the FCC Robocall Mitigation Database;
- decline to accept traffic directly from a provider that is not in the RMD or that has been removed by Commission action, consistent with applicable FCC rules;

- include contractual robocall-mitigation, traceback-cooperation, and suspension rights in interconnection or wholesale arrangements; and
- escalate, restrict, or terminate a provider relationship if illegal traffic, failed traceback cooperation, or RMD delinquency is indicated.

No upstream Account SID or third-party signing vendor is named in this plan. Supporting interconnect and platform evidence is maintained operationally and is **not** attached to this RMD PDF.

10. Traceback and law-enforcement cooperation

Peak commits to **respond fully within 24 hours** to traceback requests from the Federal Communications Commission, law enforcement, and the industry traceback consortium (Industry Traceback Group), and to cooperate with those entities in investigating and stopping any illegal robocallers that use Peak's service.

Operational practice:

- Designated traceback channel: compliance@peakmarketgrp.com and **317-303-4337**, monitored as a business-priority mailbox/line. Public contact remains contact@peakmarketgrp.com / 888-488-9069. An ITG portal login will be added to this plan when created.
- Escalation owner: Rustphine Lalas, President.
- On receiving a traceback or urgent abuse notice, Peak identifies the account, campaign, calling platform, number, traffic path, and responsible user to the extent reasonably available; preserves evidence; and responds within 24 hours with complete and accurate information.
- When a notice identifies credible evidence that consent or another lawful basis is invalid, Peak does not rely solely on a customer or lead-vendor representation. Implicated traffic is restricted or suspended while facts are reviewed.
- Corrective action may include removing records, adding suppression, changing number controls, requiring replacement evidence, ending a data source or vendor, terminating an account, and notifying affected carriers or authorities when appropriate.

Peak will not originate, carry, or continue processing traffic that it knows is illegal robocall traffic.

11. Records, training, and continuous improvement

- Records sufficient to investigate a call are retained, including account identity, campaign, calling and called numbers, date and time, route or upstream/downstream provider where known, disposition, consent or other lawful-basis evidence, and relevant configuration or user information.
- Retention is for a period appropriate to regulatory, contractual, and investigative needs. Traceback-relevant call detail is retained long enough to meet the 24-hour response commitment and subsequent investigation.
- Personnel with customer-onboarding or traffic-operations access are instructed on this program, prohibited use cases, and the duty to escalate complaints and traceback immediately.
- Violations or material risk may result in warnings, added controls, traffic limits, suspension, blocking, termination, referral to an upstream provider, or reporting to appropriate authorities.
- Peak uses complaints, traceback results, carrier notices, and monitoring outcomes to strengthen the program.

12. Regulatory history and related entities

- Individual principal named for certifications: **Rustphine Lalas, President.**
- Affiliates, parents, subsidiaries, and common control: **No.**
- Telecom DBA: **none.**
- Prior two years (FCC / law-enforcement / agency action or investigation for illegal robocalling, spoofing, or RMD-certification deficiency, for Peak and commonly owned/managed entities): **No.**

If facts change before filing, the officer must revise this section.

13. Program statement

Peak applies this program to all calls it originates or transmits. The program is designed to provide affirmative, effective, and continually improving measures to prevent Peak services from being used for illegal robocalls.

This document describes PEAK MARKETING GROUP, INC.'s program for its FCC Robocall Mitigation Database filing.