



HeyQuad LLC

24336 SUMMER NIGHTS CT, LUTZ, FL 33559

HEYQUAD.COM

david@heyquad.com

PLAN · HQ-RMP

Robocall Mitigation Plan

VERSION	EFFECTIVE	LAST REVISED	CLASSIFICATION	OWNER
3.3	2026-10-14	2026-10-14	Filing copy	David M. Hacker — Authorized Member (AMBR), sole member

1. Provider identity, contacts and service model

1.1 Identity and contacts

Field	Value
Legal name	HeyQuad LLC (as filed: HEYQUAD LLC)
Doing business as	Hey Quad (heyquad.com)
State of organization	Florida (Sunbiz document L26000372387, formed 2026-07-13)
Principal business address	24336 Summer Nights Ct, Lutz, FL 33559
FCC Registration Number (FRN)	0038863684
499 Filer ID	839247

Contact responsible for robocall mitigation, traceback and enforcement matters, as required by 47 CFR 64.6305:

Field	Value
Name	David M. Hacker
Title	Authorized Member (AMBR), sole member
Department	Compliance
Business address	24336 Summer Nights Ct, Lutz, FL 33559
Telephone	657-337-7823 (compliance line; rings the responsible officer directly)
Email	abuse@heyquad.com

The published contact address is a monitored mailbox, not a forwarding alias. Every message arriving there is stored and alerts the responsible officer on arrival, so nothing waits for anyone to open a mailbox. Senders receive an automatic acknowledgement, except automated senders and senders who have already received three acknowledgements that day, which prevents mail loops; officer alerts are rate-limited per hour and then summarized, so a flood of messages cannot bury them.

In the past two years, neither HeyQuad LLC nor any entity sharing common ownership, management, directors or control with it has been subject to any formal Commission, law-enforcement or regulatory-agency action or investigation with accompanying findings of actual or suspected wrongdoing relating to illegal robocalls, spoofing, or a deficient Robocall Mitigation Database certification or mitigation

program description. HeyQuad LLC has never had a Robocall Mitigation Database filing removed and is not prohibited from filing in the database.

1.2 The service and the customer base

Hey Quad is a hosted business phone system and AI voice receptionist sold to small businesses, initially in Florida. The dominant traffic pattern is **inbound**: a customer's published business number rings an automated receptionist or a human extension.

Outbound calling exists only in these forms:

1. A named human employee of a customer places a call from a registered desk phone, softphone or mobile app.
2. A customer's automated receptionist or call flow transfers or bridges a live inbound caller to another number.
3. The platform places calls to a customer's own staff to connect an inbound caller — ringing an agent's device or phone so the caller can be bridged to them.
4. A customer tests its own call flow or AI receptionist; a test call rings only that customer's own HeyQuad devices or one of its own telephone numbers.

We do **not** operate a predictive dialer, a campaign dialer, a lead-generation platform or a broadcast-messaging product, and we do not sell wholesale origination to other carriers or to call centers. We do not accept calls from other voice service providers for onward transmission: our only inbound source is our underlying PSTN provider, delivering calls to our own customers' numbers, so we act as neither a gateway provider nor an intermediate provider. The platform's own automated outreach to customers' contacts — appointment reminders — is **text and email only** and places no calls; see section 4.4.

HeyQuad's own business lines are operated as an account on the same platform. That operator account is not subject to the customer onboarding and verification requirements in section 3, because it is not a customer; every other control in this plan, including the automatic holds in section 5, applies to its calls.

HeyQuad does not enable predictive dialing, broadcast calling, lead generation calling, or campaign style outbound calling. Before offering any such capability, HeyQuad will conduct a separate compliance review, implement appropriate controls, and update its RMD filing as required.

1.3 Know your upstream providers

47 CFR 64.6305 and 47 CFR 64.1200(n)(3) and (n)(5) ask how a provider knows the providers whose traffic it handles.

We have exactly one provider with which we exchange traffic directly: our underlying PSTN provider Telnyx, LLC (RMD0001645), which supplies our telephone numbers and our PSTN origination and termination. Its role differs by direction:

- **Outbound**, Telnyx is the downstream provider: it receives the calls our customers originate. We are the originating provider for those calls.
- **Inbound**, Telnyx is our upstream provider: it delivers calls from the public telephone network to our customers' numbers, and we terminate them. We do not carry calls onward for other providers, sell wholesale or transit service, or accept traffic from any other provider, so we are neither a gateway nor an intermediate provider.

Our know-your-upstream-provider measures under 47 CFR 64.1200(n)(5) and 64.6305(g) are:

1. Telnyx is a direct, contracted commercial relationship in our own name, with our own account — not a chain of resellers and not an anonymous wholesale route.
2. **Robocall Mitigation Database status is checked every day.** An automated job downloads the Commission's public database export daily and confirms that Telnyx is listed and has not been removed, recording its listing, its STIR/SHAKEN status and its last recertification. Any delisting, removal or material change alerts the responsible officer, and a failed check is itself alerted rather than treated as a clean result. The same check records our own entry. If a provider we exchange traffic with directly no longer appears in the database, the responsible officer promptly confirms the status with the Commission's records and the provider and, if it is not listed, we stop accepting calls directly from that provider, as 47 CFR 64.6305(g) requires, by moving the affected traffic to another listed provider or suspending the affected service until the provider is listed again.
3. **Enforcement Bureau orders are monitored daily.** An automated job reads the Commission's docket for Final Determination Orders (EB Docket 22-174) every day and alerts the responsible officer to any new order naming a provider from which we receive traffic directly; a failed read is alerted too. If an order names such a provider, we will block and cease accepting all traffic received directly from it beginning no later than 30 days after the order's release, as 47 CFR 64.1200(n)(3) requires.
4. Inbound calls reach us only over that one provider. We do not accept SIP traffic from unknown or unauthenticated sources: our session border controller answers only for the provider trunks we have configured and for registered customer devices we have credentialed. Every inbound call is also screened against our do-not-originate list (section 4.3).
5. Illegal traffic we observe arriving from Telnyx — for example through customer complaints or the traceback process — is reported to Telnyx and, where appropriate, to the Industry Traceback Group.

If we begin exchanging traffic directly with another provider, we will apply the same measures to it, describe them here, and update the database entry within 10 business days.

2. STIR/SHAKEN implementation

HeyQuad LLC is a **voice service provider** offering interconnected VoIP service to business end users. We are **not facilities-based** for PSTN interconnection: we do not hold numbering resources directly and we do not operate our own PSTN interconnection facilities. All PSTN origination and termination is purchased from Telnyx, our underlying PSTN provider, which also supplies our telephone numbers.

HeyQuad originates its customers' calls on its own SIP platform. We therefore do **not** claim the exemption for providers that lack control over the network infrastructure necessary to implement STIR/SHAKEN: we operate the SIP elements on which STIR/SHAKEN is implemented, and we accept that 47 CFR 64.6301 applies to us.

Our STIR/SHAKEN implementation status, as that question is asked in the Robocall Mitigation Database, is **No STIR/SHAKEN implementation**, on the basis of the temporary extension in 47 CFR 64.6304(b) for providers incapable of obtaining an SPC token due to Governance Authority policy. The STI Governance Authority's SPC Token Access Policy (Policy Decision 001, v1.2) requires, among other things, a listing in the Robocall Mitigation Database and an assigned Operating Company Number (OCN). Today we meet neither, for these specific reasons:

1. **Robocall Mitigation Database listing.** This is our first filing; we are not yet listed. This filing removes that obstacle once it appears in the database.

2. **Operating Company Number.** The code administrator (NECA) assigns an OCN to an interconnected VoIP provider only on proof of service and proof of end-user customers, such as a customer contract or invoice. HeyQuad has completed its service build but has no end-user customer contract or invoice yet, so it cannot yet document a qualifying application. We will apply promptly once our first customer contract is signed.

We registered with USAC on September 9, 2026 (FCC Form 499 Filer ID 839247). On October 13, 2026 we asked the STI Policy Administrator in writing whether that registration satisfies its Form 499-A requirement and whether it accepts an OCN of the type available to us; we will follow up if we have no answer, and we will revise this explanation if the answer changes our eligibility. As soon as we are eligible we will register with the STI Policy Administrator, obtain an SPC token and an STI certificate from an approved certification authority, and sign every call we originate with our own certificate, making every attestation decision ourselves; we will also verify the authentication of signed calls we receive and apply the framework to calls carried wholly within our network. Our platform's signing function is already built and awaits the certificate, so we expect to implement promptly once we are eligible, and we will not treat the period for updating this filing as additional time to implement. We will update this filing within 10 business days of obtaining an SPC token and again when implementation is complete.

Until then, calls we originate are authenticated by our underlying provider, Telnyx, under Telnyx's own certificate and attestation policy; we do not represent this as our own implementation. All of our telephone numbers are obtained through Telnyx, and Telnyx's published policy is that numbers obtained through it receive attestation A. A forwarded call that presents the original caller's number (section 4.1) is treated under Telnyx's forwarding policy and is not represented as attestation A.

That status does not narrow this plan. Every voice service provider files a robocall mitigation plan and certifies that **all** calls it originates are subject to a robocall mitigation program, whatever its STIR/SHAKEN status. The program described in sections 3 through 8 is applied to every call we originate, on the terms stated in section 4.5. This document is that plan.

3. Customer verification

We take affirmative measures to prevent new and renewing customers from using our network to originate illegal calls, per 47 CFR 64.1200(n)(4). The controls below are **live today**.

1. **A verified email address for every owner.** Every account is created against an email address the applicant must be able to receive mail at: a verification link is sent to it and the verification is recorded on the user record. An account cannot be activated, and therefore cannot place any outbound call, until every owner of the account has verified their email address; this requirement cannot be waived or overridden by an administrator.
2. **Business identity collected at onboarding.** Legal business name, entity type, EIN (a nine-digit number, required unless the applicant is a sole proprietor), business website and industry are collected and stored on the customer account. A business cannot be recorded as verified unless a nine-digit EIN is on file and the administrator has checked it, unless the business is a sole proprietor.
3. **Business identity verified by us before any outbound call.** Before a customer can place any outbound call to the public telephone network, a HeyQuad administrator verifies the business and records the review on the customer's record. For a business found in an official business-entity registry (for a Florida business, the Florida Division of Corporations) the administrator records the registry consulted, the entity's registry number, its formation date, that its status is active, that the legal name matches, and a responsible individual at the business. The

administrator also records how the applicant's authority to act for the business was established: either the applicant is named in the registry record as an officer, manager or member (the name and role as they appear there), or the applicant has supplied a signed authorization from a named officer, manager or member of the business, which is uploaded and retained with the signer's name and title. Being named only as the registered agent is not enough on its own: that review must also carry the signed authorization. The platform refuses to record it otherwise, and a database constraint enforces the same rule. A business that cannot be found in an official registry is either verified by alternative documentation — an IRS EIN assignment letter or government-issued identification, uploaded and retained in our records together with what was checked on it — or recorded as rejected; a registered entity that is not active is recorded as rejected. The administrator also records whether the business address and telephone number were checked and the customer's stated intended use of the service. Every review is retained; the most recent one decides. **Until a verification is recorded, the server-side policy check refuses every outbound call to the public telephone network on every origination path** — this is enforced by the platform, not by the onboarding screens, and a rejected review keeps the block in place.

4. **Systematic screening before every review.** Every review is preceded by a systematic screen of the customer for an owner email address at a disposable email domain, an entity formed less than 180 days before the review (or whose formation date cannot be established), payment information whose billing name matches neither the business nor its responsible individual, whose billing country is not the United States, or that cannot be read, and a business name containing terms that imply a government agency, bank, well-known brand, carrier or charity. Screening results are recorded on the review, and a business cannot be recorded as verified until the reviewing administrator has written a resolution of each result explaining why the risk was accepted or how it was cleared; each resolution is recorded with the administrator's identity and time. The screen also flags an applicant that shares an EIN, legal name, owner email, owner telephone number or service address with a customer we have suspended, held for review or terminated.
5. **Periodic and event-driven re-verification, by risk.** Every verified customer is re-verified at least annually, and automatically whenever its ownership changes (an owner is added, removed, or gains or loses the owner role), its default payment method is replaced or removed, its authorized caller ID changes (a number is added to, moved into or reactivated on the account, or a caller-ID ownership attestation is recorded), or our traffic monitoring raises a robocall-pattern or carrier-rejection alert about it. Our operator is alerted each time. The time allowed depends on the risk: an ownership change, or an alert that placed the account on hold, refuses outbound calls to the public telephone network immediately until a new verification is recorded; a payment, caller-ID or other alert-driven change allows 7 days; the annual review allows 30 days. Emergency calls are never refused.
6. **A verified service address.** Before the account can be activated it must have a service address on file **and** an emergency location derived from it that the emergency-services provider has validated as a dispatchable address, with an emergency line identifier attached to one of the account's own numbers. An address that does not validate does not clear the gate.
7. **A payment instrument on file.** Activation requires a stored default payment method, which ties the account to a named payer. The exceptions are an account we bill by other arrangement and an account we provide on a complimentary basis, each recorded on the account.

8. **A quote we issued, and signed agreements.** Activation requires that the customer has accepted a quote issued by HeyQuad, and that every agreement we mark as required is accepted at its current version, recorded with the accepting user and timestamp.
9. **An activation gate enforced at dial time.** An organization that has not met items 1, 6, 7 and 8 and designated an on-site emergency notification contact **cannot place an outbound call at all** — the server-side policy check blocks every outbound attempt on every origination path until the account is activated. A HeyQuad platform administrator may override the address, payment, quote or agreement requirement for a specific account only with a written reason recorded against the administrator's identity; the email-verification and emergency-contact requirements cannot be overridden. A platform administrator can deactivate or suspend an organization at any time, which restores the block immediately and at the same enforcement point.
10. **Numbers are issued by us, not brought in blind.** Every telephone number a customer can select as its caller ID is provisioned in our own account with our underlying PSTN provider — bought through it or ported into it — and assigned to the customer's organization record, so every number our customers originate from is one we hold and can trace to a named account. We do not let customers present numbers held at other carriers. The one exception is forwarding a live inbound call, which may present that caller's own number (section 4.1). A ported-in number is presented only after the port completes; the platform also requires an owner's on-the-record ownership attestation before any customer-supplied number can be presented.
11. **Higher-risk calling is ours to enable, not the customer's.** International calling, calls to the Caribbean +1 area codes that bill as international, premium-rate numbers, and any increase to an account's daily outbound limits can be enabled only by a HeyQuad platform administrator. The customer cannot change these settings.
12. **Customer responsibility and termination.** Our customer agreement makes the customer responsible for all activity on the account, including by its users and anyone using its credentials, and requires use of the service in compliance with all applicable laws, including the TCPA and the FCC's rules, the Telemarketing Sales Rule, the Truth in Caller ID Act, state telemarketing and do-not-call laws. It allows us to hold outbound calling, suspend or terminate an account for suspected illegal traffic. Suspension or an outbound-calling hold is enforced at the platform level (sections 4.2, 5 and 6) and does not depend on the customer's cooperation.

4. Caller ID and outbound calling controls

Every outbound call attempt, on every origination path — call-flow dial, transfer and dial-user steps, desk-phone calls, console and API originations, queue forwards to a staff member's phone, test calls, and the platform's own monitoring call — passes a single server-side policy check before the call is placed. The check cannot be bypassed by the client: a registered device whose account uses a calling application cannot fall back to a direct platform dial when that application is unavailable; the call is refused, except calls to 911, 933, 988 and 711. These controls govern new call attempts: a hold, suspension or limit stops the next attempt, and a call already connected when it takes effect is not cut off by it.

4.1 Caller ID

Outbound caller ID cannot be supplied as free text by a customer or an API client. Every origination path resolves the presented number from the organization's own provisioned numbers: a registered device resolves through its assigned extension to an owned number, a console-placed call selects among the extension's configured owned numbers by internal identifier, and a call that rings a staff member's own

phone presents the number the caller dialed or the organization's number. A call flow can present only one of the organization's own provisioned numbers: free text, or a number the organization does not hold, is refused when the flow is published, and at call time any other value is replaced by the organization's business number before the call is placed. A device with no owned number does not dial.

A forwarded call presents the original caller's number only when we are forwarding a live inbound call from the public telephone network whose caller is on the line; on any other call it presents the organization's own number. Because every inbound call is screened against our do-not-originate list before it is routed (section 4.3), a call from a number on that list is never forwarded.

Our call platform independently refuses to originate a call whose caller ID is not a number assigned to the originating customer's account, with one exception: when a live call is transferred or forwarded, it may present the caller ID of the live call it is forwarding, and only that number. A number the customer brought to us is not presented until its ownership has been attested (section 3 item 10). This satisfies our obligation not to knowingly permit misleading caller ID under 47 U.S.C. 227(e) and 47 CFR 64.1604.

4.2 Account state and destination controls

- **Account suspension.** We can suspend an organization from the platform admin console, which immediately blocks every outbound call it attempts, at the dial-time check rather than in the user interface.
- **Outbound-calling hold.** An organization can be put on an outbound-only hold — automatically by the traffic monitoring in section 5, or by an administrator — which blocks every outbound call to the public telephone network at the dial-time check while leaving inbound service untouched. Only a HeyQuad administrator can release a hold, and the release must record what was reviewed.
- **Activation and verification gates.** An account that has not completed the requirements in section 3, or whose re-verification is overdue, cannot place an outbound call.
- **Daily outbound limits.** Each account has three daily outbound limits over the trailing 24 hours, which only a HeyQuad administrator can raise: answered minutes; call attempts, answered or not; and spend, priced at our platform rates for completed calls plus answered calls still in progress. Each limit is checked before every new call; once a limit has been reached, further calls are refused. A call already in progress is not cut off, so its final duration or cost can take the account past a limit.
- **Simultaneous-call and call-rate limits.** Each customer account has its own account on our call platform with a fixed limit on simultaneous calls and on new calls per second, set by us. Calls beyond those limits are refused by the platform, and if the platform cannot read the limit store, outbound calls to the public telephone network are refused rather than allowed.
- **Per-call fraud screening on the call platform.** Independently of the policy check above, our call platform screens every call to the public telephone network before it is connected: it blocks destinations on its built-in list of high-risk international revenue-share fraud ranges, enforces its own per-account call-rate and simultaneous-call guardrails, and scores each call for fraud risk from the account's call velocity, its simultaneous calls to high-cost destinations and the reputation of the calling source — its network address, its SIP device fingerprint and the destination number range — in a threat feed shared across all accounts on the platform. A call that scores high is held for review or blocked before it connects. Calls to 911, 933, 988 and 711 are exempt.

- **Destination policy.** International dialing is **disabled by default** for every new account. The NANP area codes that are not US or Canada — the Caribbean +1 destinations that are the classic toll-fraud pump targets — and premium 900 numbers are blocked unless the account has international dialing enabled **and** an explicit destination allowlist that matches the number. N11 and other short codes are refused, except 911, 933, 988 and 711.
- **Fail-closed checks.** The account-suspension, activation, verification and re-verification, outbound-hold, daily-limit, brought-in-number attestation, opt-out and destination-policy checks all fail closed: if a record a check needs cannot be read, the call is refused. Calls to 911, 933, 988 and 711 are decided before any record is read and are not refused by any of these checks.
- **Immutable call detail.** Every call leg is written to a call-detail record with both numbers, the originating organization, timestamps, duration and our platform's call identifier. Administrative actions are written to an audit log that the database itself makes append-only.

4.3 Consent, opt-out and do-not-originate

- **Marketing calls.** No HeyQuad product feature places marketing or promotional calls. The platform nonetheless carries a consent gate for any call marked as marketing: such a call is blocked unless a current, unrevoked, unexpired written or marketing-scope consent record exists for that recipient, is held to the recipient's local calling window and to three attempts per recipient in 24 hours, and is blocked if the consent store cannot be read. The platform cannot classify the purpose of a call a person dials by hand; our customer agreement makes the customer responsible for the lawfulness of every call its users place, including any solicitation.
- **Unified opt-out.** A recipient who texts STOP to one of a customer's numbers, or whose consent is revoked, is suppressed for **calls as well as texts** from that customer. The opt-out is kept per recipient and per customer business: it does not suppress calls from unrelated HeyQuad customers. Opt-outs are honored well inside the ten business days required by 47 CFR 64.1200(a)(10), and an opt-out survives the closure of the customer account it was collected under.
- **Do-not-originate (47 CFR 64.1200(o)).** Every call that enters or leaves our network is screened on the number it purports to originate from, and a call that matches our do-not-originate list is blocked and recorded:
 - **Inbound,** every call from the public telephone network to a customer's number is screened before it is routed. A match is rejected with a SIP 603 (Decline) before the call is answered — or, if our systems are unusually slow to decide, ended at once with a 603 cause — and is never delivered to the customer, forwarded or answered by an automated receptionist.
 - **Outbound,** the caller ID of every call we originate is screened before the call is placed, and a match is refused.

The list contains three categories, each permitted by the rule: numbers whose subscriber has asked that they never originate calls (including numbers our own customers mark as inbound-only, and requests we receive and record, with their source and date); North American numbers that are not valid; and valid North American numbers not allocated to any provider — the permanently unassignable ranges plus every central office code the North American Numbering Plan Administrator publishes as unassigned, refreshed weekly from its public data and used only while that data is current. A withheld or anonymous caller ID is not a match.

Exceptions and public-safety safeguards. We make reasonable efforts not to block calls from public safety answering points and government emergency numbers. The screen therefore does not apply in these cases:

- **A temporary protective window after a 911 call.** For 90 minutes after one of our customers' numbers places a 911 call, every incoming call to that number is delivered without DNO screening, so a public safety answering point's callback cannot be blocked. Not every call in that window is necessarily a callback; the window is a deliberate precaution, and calls delivered under it are recorded.
- **Emergency short codes as the calling number.** A call whose caller ID is 911, 933, 988 or 711 is not blocked by this screen, as a precaution: such a value is not itself proof that a public safety answering point is calling, and we treat it this way only so that no genuine emergency callback is ever blocked by a list check.
- **A never-block list.** We can exempt a public safety or government emergency number immediately.
- **A database fault.** If the list cannot be read, inbound calls are delivered unscreened rather than blocked, and the fault alerts our operator, so that a fault does not by itself cut off lawful callers or emergency callbacks.

Outside these exceptions, every inbound call is screened and a match is never delivered or forwarded. Calls placed to 911 are never blocked, as 47 CFR 64.1200(k)(5) requires; our treatment of 933, 988 and 711 is our own policy.

4.4 Automated and artificial-voice calling

The platform's own automated outreach to a customer's contacts consists of **appointment reminders sent by email and by text message**. It places no calls: there is no automated voice reminder, no automated callback calling (an AI receptionist may create a callback task for a person, who then calls as an ordinary human caller), and no artificial or prerecorded voice message delivered to a consumer by the platform. The AI receptionist answers **inbound** calls to a customer's published number and may transfer or bridge that live caller to a person; it does not originate calls to consumers. A customer's test of its own receptionist or call flow rings only that customer's own HeyQuad devices or one of its own telephone numbers.

The platform does place automated connection legs that are part of a live call — ringing a customer's own staff to connect an inbound caller, or transferring or bridging a live caller at the customer's direction. These are not standalone outreach: each exists only to connect a live caller. The only automated audio they may carry is the customer's own announcement to its staff (for example, a short "whisper" identifying the incoming call before it is connected); they deliver no marketing, informational or other recorded or artificial-voice message to consumers. The platform offers no standalone automated or artificial-voice outbound calling to third parties. Before any such capability is offered, each calling workflow must provide appropriate consent, identification of the responsible business, a valid callback number, a compliant opt-out mechanism and applicable calling-frequency controls, and this plan and the RMD entry will be updated first.

4.5 Emergency and public-service numbers

Every ordinary outbound call is subject to the controls described in this plan. Calls to emergency and designated public service numbers are handled under separate safety policies, remain associated with the calling device (or, for an automated call flow, the organization), and are logged, but are not blocked because of account status, an outbound-calling hold, a verification gate or a volume limit. Our call

platform likewise does not refuse calls to 911, 933, 988 or 711 because of account status, the simultaneous-call or calls-per-second limits, fraud screening, or a missing or unowned caller ID. When a 988 or 711 call carries no caller ID the account owns, the platform presents the account's default number, else its oldest number, and only if the account holds no number at all is the call sent as anonymous. These exemptions remove our own controls from the path; they do not guarantee completion through every network fault.

The numbers handled this way are 911, the 933 carrier test number, 988 and 711. 911 and 933 are carried on the emergency path with the dispatchable location and callback number on file for the calling device or account; 988 and 711 are carried as ordinary calls to ordinary destinations, with no emergency routing, location or on-site alert, because neither belongs on a crisis-line or relay call.

5. Traffic monitoring

- **Robocall-pattern monitoring, every 15 minutes, with automatic holds.** An automated job measures each organization's outbound calling to the public telephone network over the last hour and the last 24 hours: total attempts, the share answered, the share of answered calls that end within a few seconds, how many distinct numbers were dialed, the call rate, the volume compared with that organization's own average over the preceding seven days, and the volume of a newly activated account. A pattern consistent with robocalling — many attempts with few answers, many very short answered calls, a different number on nearly every call, or a burst of calls — raises an alert to the responsible officer. Whenever an organization is past a hard threshold and is not already on hold, it is **automatically placed on an outbound-calling hold** (section 4.2) at the same moment, so the calling stops without waiting for a person; only an administrator can release it, after review, with a written note. Every alert and hold is recorded.
- **Destination geography, calling hours and carrier rejections.** The same job also measures, for each organization: a sudden shift of its calling to destination area codes or countries it has not called in its preceding seven days; a sudden rise in calling outside the organization's own business hours compared with its usual pattern; and calls refused by the called network or party, including calls rejected as unwanted or as suspected spam. Each raises an alert to the responsible officer, and a high level of carrier rejections automatically places the organization on an outbound-calling hold.
- **The operator account is covered too.** Automatic holds apply to HeyQuad's own account on the same thresholds as any customer, because its credentials could be compromised as well; and a robocall-pattern or carrier-rejection alert about a verified customer also opens a re-verification of that customer (section 3 item 5).
- **Hourly answered-minutes tripwire.** A second job compares each organization's answered outbound minutes over the trailing 24 hours with its own daily average over the preceding seven days and alerts the responsible officer when it departs sharply, in both relative and absolute terms. It catches a compromised credential that stays under the pattern thresholds. Every alert is recorded.
- **Daily outbound limits and call-platform limits.** The per-account daily minutes, attempt and spend limits and the simultaneous-call and calls-per-second limits in section 4.2 cap what any one account can originate even before monitoring reacts.
- **Daily fair-use sweep.** A third job tracks per-seat and AI-minute consumption against per-account or platform-default thresholds and alerts before and at the threshold, which surfaces

volume that is out of character for a small-business phone line even when it is not a 24-hour spike.

- **Every refused attempt is recorded.** Every refused attempt on every origination path, including desk-phone refusals, is written once to an append-only log with the destination, its classification, the reason and the origination path; every replacement of a caller ID that was not the organization's own is recorded the same way. The platform admin console renders the most recent of these per organization, so a blocked call can be explained without a log search.
- **Alert delivery.** Monitoring alerts are delivered to the responsible officer by email.

Planned control (not certified)

The signal in this block is not monitored today and is not part of the program certified above.

1. Reputation and call-labelling warnings about our telephone numbers from third-party analytics providers. This requires a commercial monitoring service; we will update this plan and the RMD entry within 10 business days of it becoming operational.

5.1 Call analytics

47 CFR 64.6305 asks a filer to describe the call-analytics systems it uses, including any operated by a third-party vendor. Stated plainly:

We do not use a third-party call-analytics or reputation-scoring vendor. We do not buy or resell call analytics, and no vendor scores our traffic on our behalf. The analytics we use are our own:

1. **A deterministic pre-dial policy check on every origination path** (section 4). It is a rules engine, not a scoring model: account state, outbound holds, business verification and re-verification, the daily minutes, attempt and spend limits, recipient opt-out, the do-not-originate screen, caller-ID ownership, short codes and destination class are evaluated on every attempt, server-side, and the call is blocked on failure; marketing consent is evaluated for any call marked as marketing.
2. **Per-call fraud scoring on our call platform** (section 4.2). Before each call to the public telephone network connects, the platform scores it from the account's call velocity, its simultaneous calls to high-cost destinations and the reputation of the calling source — its network address, its SIP device fingerprint and the destination number range — in a threat feed built from attacks seen across every account on the platform, and holds or blocks a high-risk call before it connects.
3. **Near-real-time traffic analytics on our own call-detail records** — the robocall-pattern, geography, calling-hours and carrier-rejection monitoring, the answered-minutes tripwire and the fair-use sweep described above. The monitoring acts on its own findings: past a hard threshold it stops the account's outbound calling rather than only reporting it.
4. **Our underlying PSTN provider's own analytics.** That provider applies its own outbound fraud and traffic controls to the traffic it terminates for us. We do not see or control those controls and do not claim them as ours.

This is proportionate to the service: the dominant traffic pattern is inbound, we operate no dialer, and outbound volume per account is small enough that rule-based thresholds with automatic holds and human review are meaningful.

6. Complaint and abuse handling, and suspension

This section covers two kinds of report: complaints about traffic we originate (below), and reports from callers who believe a call to one of our customers was wrongly blocked (at the end of this section).

Complaints about traffic we originate — from a consumer, from our underlying PSTN provider, from another carrier, or from one of our own customers — are handled as follows.

1. **How a complaint is recorded.** Complaints arrive at abuse@heyquad.com, the monitored mailbox published in section 1, or at the compliance line. Every message is stored as a thread in that mailbox and alerts the responsible officer on arrival, and the sender receives an automatic acknowledgement on the terms in section 1.1. A complaint that needs investigation is logged in our request log (section 7) with its arrival time, which starts a response clock and alerts the officer before it runs out; complaints that arrive by telephone or another channel are logged the same way.
2. **How the call and the customer are identified.** The platform admin console includes a lookup that accepts a call identifier or a telephone number in any format and returns every matching call within our five-year retention period, page by page, with the originating customer, direction, both numbers, start, answer and end times, duration and disconnect cause. Because outbound caller ID is the organization's own provisioned number on every call other than a forwarded live call (section 4.1), the complained-of number identifies a candidate account. We attribute the call only after confirming it in our call-detail records against the reported time, destination and linked call legs, because an outside caller could spoof one of our numbers.
3. **Timing.** Acknowledgement of an emailed complaint is automatic. We investigate promptly and reply to a named complainant once we have reached a determination.
4. **When outbound calling is stopped.** Where the evidence is strong enough that continuing is not defensible while we investigate, the organization's outbound calling is put on hold immediately; where the investigation shows the traffic is unlawful, the organization is suspended. Both take effect at the dial-time policy check, block every outbound call the account attempts on every origination path immediately, and do not depend on the customer's cooperation. Where warranted, the customer's telephone numbers are revoked as well.
5. **When our underlying PSTN provider is notified.** Where appropriate we notify Telnyx, for example when a complaint concerns traffic that reached the PSTN over its network and we have held or suspended the customer or blocked the traffic; when Telnyx is itself the complainant, the reply to the complaint is that notification. We may also notify the provider when a complaint reveals a compromised credential on our side.
6. **How substantially similar traffic is identified.** The originating account is the anchor: the call-detail record is queried for that account's traffic over the complaint window, grouped by destination and by calling number, which shows whether the complained-of call was one of a pattern, and the account's traffic-monitoring alerts are reviewed. A hold or suspension of the account stops the whole pattern rather than the single call. Where the pattern is a destination class rather than one account, the destination policy described in section 4.2 is the control that blocks it going forward.
7. **Repeat and serious complaints.** A single substantiated complaint of a serious violation — for example a robocall campaign, spoofing, or fraud — is grounds for immediate suspension and termination. Otherwise, repeated substantiated complaints against the same customer are treated as a pattern rather than an incident, and are grounds for holding or suspending outbound calling pending a written explanation from the customer, or for terminating the account and reclaiming its numbers. A terminated or suspended customer that applies again under a new account is flagged by our screening (section 3 item 4).

8. **Retention of the record.** The complaint thread, the request-log entry, our reply, and the administrative actions taken are retained on the terms in section 8, together with the call-detail records.

Reports of erroneous blocking (47 CFR 64.1200(k)(8)). Because we block inbound calls that match our do-not-originate list (section 4.3), our public website publishes a point of contact (heyquad.com/call-blocking) for a caller who believes a call to one of our customers was wrongly blocked:

abuse@heyquad.com and the compliance line in section 1. There is no charge. We ask for the calling number, the number called, the date and time, and any tone or message heard; we find the blocked attempt in our records, check why the number matched, provide a status update within 24 hours and resolve the report within a reasonable time, as 47 CFR 64.1200(k)(8) requires. Where the block was erroneous we correct it promptly — removing a wrongly listed number or adding it to our never-block list — and tell the caller what we changed.

7. Traceback cooperation, illegal-traffic notices and cease-and-desist

We commit to **respond fully within 24 hours of receipt**, as 47 CFR 64.1200(n)(1) measures it, to all traceback requests from the Commission, from law enforcement, and from the industry traceback consortium, as required by 47 CFR 64.6305 and 47 CFR 64.1200(n)(1). Our request log keeps the response clock and alerts the responsible officer before it runs out.

Operationally: traceback requests arrive at the published contact above and alert the responsible officer. Each request is logged with its arrival time in our request log, which keeps the response deadline, alerts the officer before it runs out and again if it passes, and records what was sent and what action was taken. The lookup described in section 6 identifies the originating customer quickly, and the request log exports, for the identified call, the call detail, the caller-ID assignment of the presented number, the customer's identity and verification record and the account's recent policy decisions — never call content. We disclose call detail records to the traceback consortium in reliance on 47 U.S.C. 222(d)(2). Our internal step-by-step procedure for a traceback request is maintained as a written runbook alongside this plan.

How the traceback consortium reaches us. The Industry Traceback Group does not operate a provider self-registration list and asks providers not to register proactively. It contacts a provider using the contact information it collects from that provider's own Robocall Mitigation Database entry and from the provider's downstream partner. The contact named in section 1 of this plan is therefore the address through which traceback requests reach us, which is why it is monitored.

On a **Notification of Suspected Illegal Traffic** from the FCC Enforcement Bureau, we promptly investigate the identified traffic and report the results within the timeframe the notice specifies (the rule provides a minimum of 14 days). Our response follows our role in the identified traffic:

- **Traffic we originated** (placed by one of our customers): if it is in fact illegal we block it — by holding or suspending the originating account and, where the traffic is a destination class, by our destination policy — and cease accepting substantially similar traffic on an ongoing basis, and our report includes a certification that we are blocking it and a description of how we will identify and block substantially similar traffic going forward.
- **Traffic we received and terminated** (delivered to one of our customers by our upstream provider): our report explains that we are the terminating provider for that traffic, identifies the upstream provider that delivered it to us (Telnyx), and describes the lawful steps we are taking to mitigate it, such as adding the calling numbers to our do-not-originate list where they qualify and reporting the traffic to Telnyx and the Industry Traceback Group.

On a **carrier or private cease-and-desist notice**, we act promptly: identify the originating customer, stop the traffic where it is unlawful, and reply to the sender. The enforcement actions available to us are an immediate outbound-calling hold or suspension of the customer account, each of which blocks every outbound call at the dial-time check, plus revocation of the customer's numbers where warranted.

We cooperate with the Commission, law enforcement and other providers in investigating and stopping illegal robocallers. Our duties toward the one provider from which we receive traffic directly — Telnyx, for inbound calls — are met as described in section 1.3: its Robocall Mitigation Database listing is checked daily, Final Determination Orders are monitored and acted on under 47 CFR 64.1200(n)(3), and know-your-upstream-provider measures are taken under 47 CFR 64.1200(n)(5). If we begin exchanging traffic directly with another provider, we will apply the same measures to it and update this plan and the RMD entry within 10 business days.

Current status, stated plainly. No real traceback request has yet been received. On October 13, 2026 we rehearsed the full response process end to end against a labelled drill request in our production systems: the request was logged with its arrival time, the deadline alert reached the responsible officer by email, the lookup matched the originating customer and the exact call from the calling number, called number and call time alone, the evidence was exported, and the response was recorded within the 24-hour window and the request closed.

8. Record retention

Call detail records, customer identity and verification records, caller ID assignments, consent records, outbound-calling holds and monitoring alerts, administrative actions, complaints, and traceback materials are retained for at least five years after the applicable call, action, or termination of the customer relationship, whichever is later.

Record	Where	Retention
Call detail records	Primary database, per call	5 years, per the rule above
Refused-attempt and caller-ID replacement log	Policy-event log	5 years, per the rule above
Customer identity, business verification history, re-verification events, onboarding record, account members and roles, verified service and emergency addresses	Organization, account, verification, onboarding and member records	5 years, per the rule above
Caller ID assignments and number-ownership attestations	Number and attestation records	5 years, per the rule above; number records are kept indefinitely
Outbound-calling holds, monitoring alerts and the account's outbound policy	Hold, alert and policy records	5 years, per the rule above
Consent records and recording-disclosure evidence	Consent store, with capture source and call reference	5 years, per the rule above; opt-outs are retained indefinitely
Opt-outs and internal do-not-call	Consent and suppression store	Indefinitely, and they survive account closure
Agreements accepted, billing, payment and refund records	Agreement and billing records	7 years after termination
Administrative actions	Append-only audit log	Indefinitely; the log survives account closure
Complaints and traceback materials	Mailbox thread and the request log	Indefinitely; not affected by a customer's account closure

Customer recordings and transcripts are a separate class: they carry per-account retention limits set by the customer, or the platform default, and are purged automatically on that schedule. The records in the table above are not subject to those limits.

A deletion request does not shorten these periods. When a customer closes their account, or asks us to delete their data, the platform erases that organization's operational content: call recordings, voicemail, transcripts, message bodies, contacts and the rest of its working data. It does not erase the records in the table above. They are preserved through account closure and are deleted only when their retention period expires, by a scheduled job that runs every day; records held indefinitely are never deleted. Records are not edited after the fact: corrections are made by adding a new record, and the administrative audit log cannot be changed or deleted by the application. The platform refuses to erase a record that is still inside its retention period. The only exception is a platform administrator's forced override, recorded with a written reason against the administrator's identity, which we use solely to remove a test account or an account opened in error that never carried customer traffic. No record subject to a legal hold is erased while the hold is in place.

9. Governance, recertification and certification

Obligation	Deadline
Annual recertification that RMD information is true and correct	On or before March 1 each year, every year, by every filer
Update the RMD after any change to filed information	Within 10 business days
Review this plan	At least annually, before recertifying
Respond to a traceback request	Within 24 hours of receipt as 47 CFR 64.1200(n)(1) measures it (section 7)
Report of erroneous blocking	Status update within 24 hours; resolved within a reasonable time (47 CFR 64.1200(k)(8))
Investigate an abuse complaint	Promptly
Act on a cease-and-desist notice	Promptly

The responsible officer named in section 1 owns this plan, reviews it before each March 1 recertification, and updates it whenever a control described here is added, removed or materially changed. A filing that has gone out of date is itself a violation, so the 10-business-day update window is treated as a hard deadline and not a target.

Recertification is an affirmative annual act. A filing left untouched is not recertified, and an entry that is not recertified may be removed from the database — at which point other providers are required to stop accepting our traffic.

Certification

I certify under penalty of perjury that I am an officer of HeyQuad LLC authorized to make this certification, that I have read this Robocall Mitigation Plan, that it accurately describes the robocall mitigation program applied to all calls originated on our network, and that the information submitted to the Robocall Mitigation Database is true, accurate and correct.

Field	Value
Signature	/s/ David M. Hacker
Name	David M. Hacker
Title	Authorized Member (AMBR), sole member
Date	2026-10-14

24336 Summer Nights Ct, Lutz, FL 33559 · 657-337-7823 · abuse@heyquad.com