

# ROBOCALL MITIGATION PLAN

STIR/SHAKEN | KYC | TRACEBACK | RESPONSE

|                                |                                           |
|--------------------------------|-------------------------------------------|
| Legal company name             | GRADIENT CONNECT LLP                      |
| FCC Registration Number (FRN)  | 0038736336                                |
| RMD filing number              | [RMD NUMBER]                              |
| Operating Company Number (OCN) | [OCN]                                     |
| 499 Filer ID                   | 839224                                    |
| Principal business address     | 1801 West End Ave, Nashville, TN 37203    |
| Company website                | gradientconnect-ai.com                    |
| Plan version                   | 1.0                                       |
| Effective date                 | September 23, 2026                        |
| Company Officers               | Matthew Yeazel , CEO<br>James Persky, CEO |

*Company-controlled compliance plan — validate all company facts before submission.*

## 1. Plan governance and accuracy standard

GRADIENT CONNECT LLP (the "Company") maintains this Robocall Mitigation Plan as an accurate statement of its current robocall-mitigation controls and filing commitments. Company-specific fields are completed from verified records. This Plan, the Robocall Mitigation Database (RMD) portal entry, the CORES record, customer contracts, network implementation, and operating procedures are maintained consistently with one another. The signing officer approves the filing under penalty of perjury.

### Governance principles

- Identify — maintain the legal entity, FRN, RMD number, OCN, business names, provider roles, affiliates, principals, and contact information.
- Scope — describe only the provider roles, network status, and operational controls that accurately apply to the Company.
- Substantiate — support each control with actual procedures, tools, responsible teams, review cadence, escalation criteria, and retained evidence.
- Reconcile — keep this Plan aligned with the RMD portal, CORES, contracts, STIR/SHAKEN implementation status, and current operations.
- Approve — require review by operational owners, the regulatory owner, and the signing company officer before submission.
- Protect — use the public version unless confidential treatment is legally justified and requested through the FCC's required process.

## 2. Company identity and document control

|                                       |                                        |
|---------------------------------------|----------------------------------------|
| <b>Legal company name</b>             | GRADIENT CONNECT LLP                   |
| <b>DBA / other business names</b>     | Gradient Connect LLP, Gradient Connect |
| <b>Entity type</b>                    | PARTNERSHIP                            |
| <b>State of formation</b>             | TN                                     |
| <b>FCC Registration Number (FRN)</b>  | 0038736336                             |
| <b>RMD filing number</b>              | [RMD NUMBER]                           |
| <b>Operating Company Number (OCN)</b> | [OCN]                                  |
| <b>Principal business address</b>     | 1801 West End Ave, Nashville, TN 37203 |
| <b>Company website</b>                | gradientconnect-ai.com                 |

### Responsible contacts

| Role | Name / title | Business email | Telephone |
|------|--------------|----------------|-----------|
|------|--------------|----------------|-----------|

|                  |                |                              |             |
|------------------|----------------|------------------------------|-------------|
| RMD / regulatory | Matthew Yeazel | sales@gradientconnect-ai.com | 19514452271 |
| Traceback / ITG  | Matthew Yeazel | sales@gradientconnect-ai.com | 19514452271 |
| Legal process    | Matthew Yeazel | sales@gradientconnect-ai.com | 19514452271 |
| Security / fraud | Matthew Yeazel | sales@gradientconnect-ai.com | 19514452271 |

Control reminder: RMD and CORES information must be reviewed whenever this document changes. Current rules require updates to specified filing information within ten business days of a change, and annual RMD recertification on or before March 1.

### 3. Executive statement and core commitments

GRADIENT CONNECT LLP submits this Robocall Mitigation Plan in connection with its certification in the Federal Communications Commission's Robocall Mitigation Database. This Plan describes the specific reasonable steps the Company uses to prevent, detect, investigate, mitigate, and stop illegal robocalls that may originate, transit, or otherwise be processed on its network.

The Company has tailored these measures to its role or roles in the call path, network architecture, customer base, services, and risk profile. The Company reviews this Plan when its operations, regulatory obligations, or mitigation controls materially change.

#### Core commitments

- Reasonable steps — apply and document specific controls intended to significantly reduce the origination, carrying, or processing of illegal robocalls.
- Twenty-four hour response — respond within 24 hours to traceback requests from the FCC, law enforcement, and the industry traceback consortium.
- Cooperation — cooperate in investigations and take appropriate action to stop illegal robocallers using the Company's services.
- Accurate filing — maintain complete and current RMD information, complete annual recertification, and promptly implement required updates.

#### Company-specific statement

[Describe why the selected controls are reasonable for the Company. Address provider role, network scale, customer types, traffic profile, geographic footprint, technology stack, and prior compliance experience. Avoid generic language that merely repeats the rule.]

### 4. Provider role and network profile

|                                               |                              |
|-----------------------------------------------|------------------------------|
| <b>Provider roles (select all that apply)</b> | VOICE SERVICE                |
| <b>Traffic served</b>                         | [WHOLESALE / RETAIL / BOTH]  |
| <b>Geographic scope</b>                       | USA                          |
| <b>Services</b>                               | [VOICE / VOIP / SMS / OTHER] |
| <b>Network environment</b>                    | [IP / NON-IP / HYBRID]       |

### Position in the call path

[Identify the typical source of traffic, direct upstream and downstream relationships, where calls enter and leave the Company's network, which party assigns telephone numbers, which party performs call authentication, and where the Company can block, label, redirect, or terminate traffic.]

Role-specific scope: provider obligations and operational controls differ by call-path role. This Plan applies only to the controls the Company actually performs and does not imply control over functions handled exclusively by another provider.

## 5. Call authentication — STIR/SHAKEN

|                                       |      |
|---------------------------------------|------|
| <b>Implementation status</b>          | FULL |
| <b>Extension or exemption claimed</b> | N/A  |
| <b>Own SPC token and certificate</b>  | YES  |

### Authentication controls

- Authenticate entity — verify the customer's legal identity, authority, ownership, and contact information.
- Validate number rights — confirm the customer's legitimate right to use each asserted calling number.
- Assign attestation — apply documented criteria consistent with the authenticated relationship and number authorization.
- Monitor use — review calling behavior, complaints, tracebacks, and changes that may undermine prior verification.

### Company-specific description

[Describe how the Company determines and records each attestation decision, its use of its own SPC token, certificate and key controls, and its handling of non-IP segments, unsigned traffic, re-verification triggers, and exceptions.]

Required implementation statement: FULL means the Company's entire voice network is IP and it authenticates all applicable calls with its own SPC token and certificate. PARTIAL means it authenticates all applicable calls on the IP portion of its network and identifies a valid extension or exemption for the remainder. NONE requires a

valid extension or exemption and a specific explanation. If a third party performs signing, the Company still makes every attestation decision and uses the Company's own certificate.

## 6. Customer onboarding and know-your-customer controls

- Identity and authority — legal name, formation documents, address, beneficial ownership or principals as appropriate, authorized signer, and reliable contact channels.
- Business legitimacy — website and public presence, service purpose, regulatory or licensing status where relevant, sanctions or enforcement screening, and reputation review.
- Number authorization — inventory of calling numbers, assignment or authorization evidence, intended caller-ID presentation, and control over delegated numbers.
- Traffic profile — expected use case, campaign type, calling geography, traffic volume, average duration, answer rate, complaint sensitivity, and upstream/downstream relationships.
- Contract controls — prohibitions on unlawful calls and spoofing, audit and information rights, traceback cooperation, suspension rights, and prompt change notification.
- Ongoing review — risk-based re-verification, trigger events, periodic screening, number changes, unusual traffic, complaints, tracebacks, and ownership changes.

Provider-role requirement: as a voice service provider, the Company applies affirmative, effective measures to prevent new and renewing customers from originating illegal robocalls and knows its end-user customers as required by 47 C.F.R. § 64.1200(n)(4). As a gateway or non-gateway intermediate provider, the Company knows its immediate upstream providers as required by § 64.1200(n)(5). Retain only the statement matching each role reported in the RMD.

## 7. Traffic analytics, monitoring and investigation

|                                        |           |
|----------------------------------------|-----------|
| <b>Call analytics used</b>             | YES       |
| <b>Monitoring cadence</b>              | REAL-TIME |
| <b>Systems or third-party vendors</b>  | NONE      |
| <b>Underlying provider relied upon</b> | NONE      |

### Indicators reviewed

Call volume and velocity; answer-seizure ratio; average call duration; short-duration concentration; number rotation and spoofing signals; complaint and traceback history; geographic anomalies; campaign and customer risk.

### Investigation workflow

1. Alert — analytics, complaint, provider notice, traceback, or law-enforcement request.
2. Triage — validate data, assess urgency, identify customer and call-path relationships.

3. Investigate — review CDRs, customer profile, number rights, campaign purpose, and history.
4. Act — block, label, rate-limit, warn, suspend, terminate, or escalate as appropriate.
5. Document — record evidence, rationale, communications, outcome, and follow-up date.

Required analytics disclosure: state expressly whether call analytics are used. Describe each Company-operated or third-party analytics system, the data and indicators reviewed, cadence, alert routing, investigation owner, and decision authority. If the Company relies on an underlying provider's analytics, identify that provider and explain the reliance.

## 8. Blocking, remediation and enforcement

- Observe — increase monitoring, validate the alert, preserve records, and compare activity to the approved customer profile.
- Inquire — request an explanation, campaign documentation, consent evidence, number authorization, and corrective-action plan.
- Restrict — apply targeted blocking, rate limits, labeling, routing restrictions, or temporary suspension while risk is assessed.
- Terminate — suspend or terminate service, block affected traffic, notify relevant partners, and escalate as legally appropriate.

The Company's agreements prohibit illegal, fraudulent, misleading, spoofed, or otherwise unauthorized calling. Subject to applicable law and contract terms, the Company may deny, block, restrict, suspend, or terminate service when traffic presents an unacceptable risk, violates the Company's policies, or is not promptly remediated.

### Company decision rules

[Describe when warnings are appropriate; when immediate blocking or suspension is permitted; who approves termination; how customer explanations are evaluated; how affected providers are notified; and how the Company verifies that remediation was effective.]

## 9. Upstream and downstream provider diligence

- RMD screening — verify that direct providers appear in the RMD and are not identified as removed or ineligible before accepting traffic, as applicable.
- Identity and ownership — collect legal-entity, address, control-person, affiliate, service, and contact information appropriate to the relationship.
- Mitigation review — review the provider's role, mitigation plan, STIR/SHAKEN status, traceback practices, customer-vetting approach, and enforcement history.
- Contract terms — require lawful traffic, accurate identity information, traceback cooperation, information rights, prompt incident notice, and suspension or termination remedies.
- Ongoing monitoring — monitor traffic patterns, complaints, traceback performance, routing changes, reputation signals, and material changes to the provider's RMD filing.

- Escalation — define when traffic will be blocked, rerouted, limited, suspended, or rejected and who may authorize emergency action.

|                              |                             |
|------------------------------|-----------------------------|
| <b>Screening owner</b>       | James Perksy, CEO           |
| <b>Review cadence</b>        | [ENTER]                     |
| <b>RMD evidence retained</b> | [SCREENSHOT / EXPORT / LOG] |
| <b>Escalation contact</b>    | [ENTER]                     |

## 10. Traceback response

The Company commits to timely, complete cooperation and maintains an operational process capable of meeting the 24-hour response requirement.

1. Receive — a monitored mailbox or portal routes the request to the designated contact and backup.
2. Validate — confirm request source, identifiers, call example, date/time/time zone, and required response format.
3. Research — locate CDRs, ingress/egress provider, customer, number, identity headers, and relevant case history.
4. Respond — provide an accurate response through the authorized channel within 24 hours; escalate gaps immediately.
5. Remediate — investigate suspicious traffic, preserve records, act on customer/provider risk, and document closure.

|                                     |                                   |                              |             |
|-------------------------------------|-----------------------------------|------------------------------|-------------|
| <b>Primary traceback contact</b>    | Matthew Yeazel                    | sales@gradientconnect-ai.com | 19514452271 |
| <b>Backup / after-hours contact</b> | Matthew Yeazel                    | sales@gradientconnect-ai.com | 19514452271 |
| <b>Systems searched</b>             | [CDR / SIP / ROUTING / CASE DATA] |                              |             |
| <b>Response evidence retained</b>   | 7 Years                           |                              |             |

## 11. Law enforcement and regulatory requests

The Company will cooperate with valid requests from the FCC, law-enforcement agencies, and other authorized governmental entities. The Company will verify the request, consult counsel when appropriate, preserve relevant records, and disclose only information authorized by applicable law and the legal process presented.

### Request intake

- Agency and requestor identity
- Official contact information
- Legal authority and scope
- Target numbers / accounts
- Date, time, and time zone
- Return deadline and secure channel

### Validation and response

- Authenticate the requestor independently
- Confirm legal sufficiency and jurisdiction
- Limit collection to authorized scope
- Preserve responsive records
- Obtain required internal approval
- Transmit securely and document completion

Legal review required: customize this section for the Company's services, applicable privacy and CPNI obligations, geographic reach, data-retention practices, emergency-disclosure process, and procedures for subpoenas, court orders, warrants, civil investigative demands, and regulatory inquiries.

## 12. Incident, enforcement and corrective-action history

Provide accurate, date-bounded responses. Do not use an absolute "none" statement unless it has been verified across the Company, relevant affiliates, and principals.

|                                                                |                    |
|----------------------------------------------------------------|--------------------|
| <b>Relevant traceback requests during review period</b>        | NONE               |
| <b>FCC or law-enforcement investigations</b>                   | NONE               |
| <b>Enforcement actions concerning illegal robocalls</b>        | NONE               |
| <b>RMD removals, deficiencies, or cure requests</b>            | NONE               |
| <b>Material customer/provider terminations</b>                 | [NUMBER / SUMMARY] |
| <b>Affiliates or principals implicated in relevant matters</b> | NONE               |

## 13. Governance, training and records

- Ownership — executive sponsor, regulatory owner, operational owner, legal reviewer, traceback contact, and backup responsibilities.
- Training — role-based onboarding and recurring training for sales, provisioning, network operations, fraud, support, compliance, and legal teams.

- Records — document retention for KYC, number authorization, CDRs, alerts, investigations, customer communications, tracebacks, and legal requests.
- Testing — periodic sampling, tabletop exercises, response-time testing, control review, escalation testing, and documented remediation.

#### **Required review triggers**

- Annual RMD recertification on or before March 1
- Change to required RMD or CORES information
- New provider role, service, market, affiliate, or ownership structure
- Material change to STIR/SHAKEN implementation or certificate operations
- Significant traceback, complaint, enforcement, or fraud event
- Change to monitoring, blocking, KYC, routing, or outsourced compliance controls

|                                  |                          |
|----------------------------------|--------------------------|
| <b>Plan review frequency</b>     | Within 10 days of change |
| <b>Record retention schedule</b> | 7 Years                  |

Ten-business-day control: assign an owner and monitoring mechanism for changes that require updates to the RMD or CORES. Document the date the change occurred, date identified, responsible approver, and date the update was completed.

## 14. Officer review and approval

Draft attestation — counsel review required.

I am authorized to approve this Robocall Mitigation Plan on behalf of GRADIENT CONNECT LLP. I have reviewed the Plan and, to the best of my knowledge after reasonable inquiry, the information it contains is true, accurate, complete, and consistent with the Company's current operations. The Company will implement and maintain the measures described, respond to qualifying traceback requests within 24 hours, cooperate with authorized investigations, update required filing information within applicable deadlines, and complete required annual RMD recertification. I agree to update this RMD within 10 days of a traceback.

|                                |                              |
|--------------------------------|------------------------------|
| <b>Authorized officer name</b> | Matthew Yeazel               |
| <b>Officer title</b>           | CEO                          |
| <b>Business email</b>          | sales@gradientconnect-ai.com |
| <b>Business telephone</b>      | 19514452271                  |
| <b>Approval date</b>           | September 23, 2026           |
| <b>Effective date</b>          | September 23, 2026           |

Officer signature: \_\_\_\_\_ Date: \_\_\_\_\_

## Appendix A — Pre-filing checklist

- Legal name, FRN, address, business names, roles, OCN, affiliates, principals, and contacts match the RMD portal and CORES.
- STIR/SHAKEN implementation status and any extension or exemption language are accurate.
- The plan contains specific reasonable steps used by the Company — not generic promises or copied rule text.
- The 24-hour traceback commitment, designated contacts, backup coverage, systems, and escalation process are operational.
- KYC, traffic analytics, blocking, provider diligence, and enforcement descriptions match current procedures and contracts.
- Investigation and enforcement disclosures have been verified across the Company, relevant affiliates, and principals.
- No confidential customer, network, credential, or investigative information appears in the public version.
- Every company-specific completion field is resolved; officer approval is complete.
- The update owner understands the ten-business-day requirement and annual March 1 recertification process.

### Primary reference set

- 47 C.F.R. § 64.6305 — Robocall mitigation and Robocall Mitigation Database requirements.
- FCC, Robocall Mitigation Database Report and Order, FCC 24-135.
- FCC Wireline Competition Bureau, DA 26-72 — effective dates, annual recertification, and filing guidance.
- FCC, Robocall Mitigation Database Filing Instructions.
- FCC, RMD Frequently Asked Questions.
- USTelecom Industry Traceback Group provider resources.

Regulatory status: company facts, practices, and filing representations must be independently verified, and current FCC requirements should be checked immediately before each filing or recertification.