

Robocall Mitigation Database (RMD) Certification & Mitigation Plan

1. Company Information

- Company Name: Dega Systems Inc
- Operating Name (DBA): Dega Systems
- FRN (FCC Registration Number): 0031719438
- Contact Person: Hector Ortiz hector@degasystems.com
- Role in Call Chain: Originating

2. Certification

We certify that:

- Our company is an originating voice service provider that offers VoIP and SIP-based voice services solely as part of managed IT services for our business clients.
- Our company **does not perform STIR/SHAKEN authentication or call signing itself**. Instead, **all eligible outbound IP-based calls originated by our customers are authenticated and signed by our upstream voice service providers**, including but not limited to Bandwidth and SIPTrunk.com, in accordance with FCC STIR/SHAKEN requirements.
- Because STIR/SHAKEN authentication is fully performed by our upstream providers on our behalf, **our company is not required to obtain or rely upon a STIR/SHAKEN implementation extension or exemption**.
- Attestation levels for outbound calls are assigned by our upstream carriers based on their direct relationship with the calling number, calling party, and source of the traffic.
- Our company does not maintain its own STIR/SHAKEN signing infrastructure, Service Provider Code (SPC), certificate authority credentials, or authentication tokens.
- We have implemented **reasonable and effective robocall mitigation measures** appropriate to our size, role, and technical capabilities, including robust customer vetting, continuous traffic monitoring, fraud detection, and prompt response to suspected unlawful call activity.
- We do not knowingly or negligently originate, facilitate, or transmit unlawful robocall traffic, and we maintain documented internal procedures to prevent, detect, investigate, and remediate such activity.
- We cooperate fully with the FCC, law enforcement agencies, and the Industry Traceback Group in investigating and mitigating unlawful robocall activity.

- We will update this certification and our Robocall Mitigation Plan within ten (10) business days of any material change to our upstream carrier relationships, STIR/SHAKEN handling, or robocall mitigation practices.

3. Robocall Mitigation Measures ○

STIR/SHAKEN Deployment

We provide VoIP services using upstream carriers Bandwidth and SIPTrunk.com, who apply full STIR/SHAKEN signing on all eligible SIP calls. Our company does not originate calls directly on the PSTN and does not maintain its own SPC token, certificate authority, or STIR/SHAKEN signing infrastructure.

For calls that are not eligible for STIR/SHAKEN (e.g., TDM interconnects), we rely on our upstream carriers' mitigations.

We maintain strong customer vetting, require valid business identification, monitor call patterns, and investigate any suspicious traffic. We enforce strict AUPs, block illegal robocalling, and cooperate with traceback requests

3.2 Traffic Monitoring

Our company provides voice services only as part of managed IT solutions for our business clients. We do **not** offer wholesale voice termination or high-volume calling services. As part of our robocall mitigation program, we implement the following controls:

- **Continuous traffic monitoring** to identify unusual calling patterns, including short-duration spikes, high-volume bursts, unexpected international traffic, or other anomalies inconsistent with the customer's normal profile.
- **Automated analytics** through our upstream voice providers (e.g., Bandwidth, SIPTrunk) and internal monitoring tools to detect potential robocall behaviors.
- **Daily review of call analytics** by our security/compliance staff. Alerts from upstream carriers are investigated immediately.
- **Immediate suspension procedures** for any suspected abusive or suspicious traffic until review is completed.

○ **Call Vetting & Onboarding**

We only provide voice services to existing or contracted **Managed IT Services (MSP) clients**, and **do not** sell phone services to general public, resellers, or wholesale voice customers. As part of our onboarding process:

- **Business Verification:**

We collect and verify valid business information, including state business registration, EIN/tax ID, and authorized representative details.

- **Corporate Validity Check:**

Corporate existence is verified through Secretary of State databases or equivalent public registries.

- **Use-Case Review:**

We review the customer's expected calling patterns, business purpose, and use cases to ensure they align with our acceptable-use policies.

- **Risk Screening:**

Customers are screened against publicly available industry risk indicators (e.g., FCC enforcement actions, traceback consortium data, known bad-actor patterns).

- **Restricted Client Base:**

We only support phone services for managed IT clients with standard business calling needs. We do **not** provide service to high-risk verticals, call centers, lead generators, or outbound-heavy telemarketing operations.

Ongoing Monitoring:

- Re-verify customer information on an annual basis.
- Continuously monitor call patterns for anomalies, including short-duration calls, high calls-per-second spikes, and international origination.
- Customers generating high-volume or potentially high-risk traffic undergo additional vetting and may have call signing handled through our upstream SIP provider.
- We maintain awareness of STIR/SHAKEN partial implementation requirements and rely on our upstream carrier for full attestation and certificate signing where applicable.
- Any detected suspicious or potentially unlawful traffic is investigated, and mitigation actions are applied as appropriate.

- **Remediation:**

- Escalate suspicious accounts for **manual review**.
- Suspend or terminate customers if they fail remediation or exhibit high-risk traffic.

- Report identified unlawful robocall traffic to the **Industry Traceback Group** within 24 hours.
- For traffic signed via upstream carriers (partial STIR/SHAKEN), ensure attestation levels are **monitored** and any anomalies are flagged for further investigation.
- Maintain records of remediation actions and communications for regulatory and internal compliance purposes.

○ **Active Blocking / Quarantine**

- Suspected unlawful robocall traffic is **blocked, rate-limited, or quarantined** for internal review.
- Coordinated response with **Industry Traceback Group** requests within 24 hours.
- Traffic signed through upstream carriers (partial STIR/SHAKEN) is **monitored for attestation anomalies**, and any suspicious patterns are subject to additional mitigation actions.
- Maintain logs of all blocked or quarantined calls for regulatory review and internal auditing.

- **Complaint Handling** ○ Dedicated abuse reporting email/portal: [support@degasystems.com] ○ Consumer complaints investigated within 24–48 hours. ○ Remediation steps may include customer suspension or termination.

4. **Compliance & Enforcement** ○ Staff trained annually on FCC robocall mitigation rules. ○ Periodic internal audits of traffic analytics and customer compliance. ○ Documentation retained for minimum of two years for regulatory review.

5. **Point of Contact for FCC & Industry Traceback** ○ Name: Hector Ortiz ○ Title: CEO
○ Email: Hector@degasystems.com ○ Phone: 6463501531

6. Submission

This plan will be uploaded to the FCC Robocall Mitigation Database (RMD) and updated promptly upon material changes.