

Dataspindle LLC — Robocall Mitigation Program

****WE DO NOT authorize individuals or businesses to use information found here to solicit to us. All requests will be ignored and reported where appropriate****

David Sgro, President — 302-448-4988 x150 — dave@dataspindle.com

Robocall Mitigation Program – Dataspindle LLC

Date: September 23, 2025

Provider & Filing Details

Provider: Dataspindle LLC

FRN: 0026522417

Traceback / Enforcement POC (24/7): David Sgro, President — 302-448-4988 x150 — dave@dataspindle.com

Date: September 23, 2025

1. Scope & Compliance Posture

Dataspindle is a reseller of PSTN-enabled VoIP services from upstream providers Bandwidth and Flowroute to U.S. business customers only. We sell phone services exclusively to existing IT service clients, with no exceptions and no sales to consumers. We do not own or operate any PBX, network infrastructure, or other telecommunications equipment. Customers own their PBXs at their locations and connect directly to Bandwidth or Flowroute for all call origination and routing. We handle billing and support but do not originate calls ourselves. We do not operate as a foreign gateway provider. We maintain and update this program and our Robocall Mitigation Database (RMD) filing in accordance with applicable FCC rules.

1. Caller ID Authentication (STIR/SHAKEN)

Implementation: As a reseller lacking any network infrastructure or control necessary to implement STIR/SHAKEN, Dataspindle is exempt from the STIR/SHAKEN implementation obligation under FCC rules (47 CFR § 64.6301 and FCC Order 24-120). We do not sign or authenticate calls ourselves and do not possess our own Service Provider Code (SPC) token or certificate. Instead, we rely on our upstream providers (Bandwidth and Flowroute), who have fully implemented STIR/SHAKEN on their networks, to authenticate all IP-originated outbound calls in compliance with FCC requirements.

Hosted signing support: Calls are signed on our upstream providers' signing platforms (Bandwidth and Flowroute) in accordance with their policies and our attestation determinations.

Our upstream providers apply the signatures and perform additional network-layer analytics/mitigation where appropriate.

Legacy interconnects: Where end-to-end SHAKEN cannot be preserved due to TDM/legacy routing, we apply the mitigation controls in Sections 3–6 and prefer interconnects that preserve identity headers.

1. Know-Your-Customer (KYC) & Onboarding

Prior to enabling outbound service or new campaigns, Dataspindle takes affirmative, effective measures to prevent unlawful robocalls, including:

- Meeting every customer in person to verify business identity (legal name, address, responsible contacts).
- Verification of EIN and, where appropriate, credit checks conducted internally through manual review of provided documents.
- Right-to-use number verification for every CLI (LOA, inventory proof, or verified assignment) conducted via direct checks with our upstream providers (Bandwidth and Flowroute).
- Use-case review, expected volumes/CPS, calling hours/geographies.
- Customer acknowledgment of TCPA/TSR/state-law obligations (consent, opt-out, DNC) via signed agreements.
- Heightened review or denial for high-risk verticals.

Dataspindle does not use third-party vendors for KYC analytics; all verification is performed internally through manual processes. We also interconnect only with providers that have current, non-delisted RMD certifications.

1. Attestation Policy (A-Only)

Dataspindle provides information to our upstream providers to enable A (Full) attestation exclusively, but the final attestation and signing are performed by Bandwidth and Flowroute.

- We confirm the customer's identity and the customer's authorized control/ownership of each calling number prior to use.
- We do not permit customers to send caller ID that is not owned or authorized for their use.
- If number association cannot be verified to A-level standards, the traffic is not enabled (we do not pass or enable such calls).
- We never enable B or C attestation and do not act as a foreign gateway.

1. Ongoing Traffic Monitoring & Analytics

We continuously monitor outbound traffic (automated and manual review) for indicators of unlawful or abusive activity, including:

- High short-duration/zero-duration ratios; unusual CPS spikes; anomalous geo patterns.
- Invalid/unassigned/unallocated ANIs and calls to Do-Not-Originate (DNO) ranges.
- Complaint signals, negative reputation labels, or carrier/partner alerts.

Dataspindle does not use additional third-party vendors for traffic analytics beyond our upstream providers; Bandwidth and Flowroute operate additional analytics, including real-time traffic monitoring, anomaly detection, and mitigation tools, and may take independent mitigation steps consistent with their policies.

Page 2:

1. Mitigation, Blocking & Enforcement

When indicators suggest unlawful or harmful traffic, we act rapidly to:

- Contain: throttle, suspend, or block specific CLIs/routes/customers; block invalid, unallocated, or unassigned caller IDs and DNO ranges in coordination with Bandwidth and Flowroute.
- Investigate: contact the customer promptly for campaign details and consent evidence; require remediation (list scrubs, cadence fixes, caller-ID corrections).
- Enforce: terminate service for non-compliance; coordinate with upstreams to quarantine traffic during investigations.

We review efficacy and false positives periodically and adjust controls as needed.

1. Traceback & Law-Enforcement Cooperation

Dataspindle responds within 24 hours to traceback requests and cooperates fully with the FCC, law enforcement, and the Industry Traceback Group to identify and stop illegal traffic.

We rely on our upstream providers to facilitate with this

1. Recordkeeping

We retain relevant CDRs, SIP traces, signing/attestation metadata, and investigation notes for a minimum of 12 months (longer where required by law or contract).

1. Enforcement History (past two years)

Dataspindle LLC's certification was removed from the Robocall Mitigation Database by the FCC Enforcement Bureau on August 6, 2025, and August 25, 2025, due to deficiencies in the Robocall Mitigation Database certification or mitigation program description, including inadequate details, inconsistencies, or failure to update in a timely manner after notifications. No findings of actual or suspected wrongdoing involving transmitting, encouraging, assisting, or facilitating illegal robocalls or spoofing were made. The filings were provisionally reinstated on August 29, 2025, pending corrections. Dataspindle LLC has not been subject to any other formal actions or investigations by the Commission, law enforcement, or regulatory agencies in the prior two years.

1. Program Governance & Updates

This program is owned by Compliance/Operations with executive oversight by the President. We periodically audit attestation logic, monitoring thresholds, and KYC artifacts, and we update our RMD filing promptly when material information changes.