DepositLeads Vendor-Risk Packet
Generated 2026-06-14
Purpose: help bank executives, compliance teams, and vendor-risk teams understand controls before beta or procurement

SOC 2 Roadmap

- Phase 1: formalize access control, change management, vendor review, incident response, and evidence retention.
- Phase 2: collect 90 days of audit evidence for production access, deployments, monitoring, backups, and support procedures.
- Phase 3: complete readiness assessment, remediate gaps, then enter Type I followed by Type II observation.

Data Source Register

- Sources are classified as public/permitted, licensed/vendor, bank-provided, or derived/cohort.
- Each module should display source type, last successful run, expected cadence, records added this week, and freshness SLA status.
- Truth Audit snapshots and source URL liveness runs are retained so bank reviewers can inspect 30-day source-proof history.
- News and social inputs use public RSS/Atom feeds or approved provider APIs only; no private groups, DMs, or logged-in scraping.

Suppression Policy

- Banks may upload customer, opt-out, DNC/TCPA, and policy suppression files before banker outreach.
- Exact matches are suppressed automatically; fuzzy matches route to admin review.
- Suppressed leads are excluded from call queues and default exports; override exports require role permission and audit reason.

GLBA / FCRA Posture

- DepositLeads is a business development and public-record intelligence workflow, not a credit decisioning or prescreening engine.
- The product should not state or imply credit eligibility, payoff amounts, account balances, or primary-bank certainty.
- Consumer mortgage/mover/probate use requires licensed/permitted source terms, suppression, and careful banker language.

Security Architecture

- Role-gated app routes, organization-scoped data access, production auth keys, export audit logs, and admin-only setup controls.
- Secrets live in deployment environment variables; vendor credentials are not exposed to client-side code.
- Every export, CRM sync, account-opened match review, and core-attribution webhook should write an audit trail with user, timestamp, filters, row count, and reason.

Disaster Recovery
- Database backups should run daily with point-in-time recovery where the managed database supports it.
- Exports and uploaded suppression files should be retained in durable object storage with lifecycle rules.
- Target recovery posture: RPO under 24 hours for beta, RTO under 8 business hours, with quarterly restore tests before scale.

Model Contract Terms
- Customer owns bank-provided data, suppression files, CRM notes, and banker activity data.
- DepositLeads may process customer data only to provide the subscribed service and support authorized bank users.
- No resale of bank customer lists, no cross-bank data pooling, and termination includes export plus deletion/retention schedule.

Insurance / Cyber Overview
- Maintain cyber liability, technology E&O, and general liability coverage sized for bank vendor expectations.
- Provide certificate of insurance during bank due diligence and renew annually.
- Incident notification, breach cooperation, and subprocessor disclosure should be included in contract exhibits.

Uptime / Freshness SLA
- Daily public-source feeds alert after 3 days stale; weekly or licensed-provider feeds alert after 7 to 8 days stale.
- Every module should show 30-day run history, uptime percentage, last successful run, expected cadence, stale status, and records added this week.
- Stale feeds remain visible with warnings rather than hiding data age from bankers.

CRM / Core Integration Controls
- HubSpot, Salesforce, and nCino connections are designed as bidirectional syncs with visible field mapping and server-side credentials.
- Low-confidence core account-opened events route to a human match-review queue before ROI attribution changes.
- Suppression state, source proof, banker owner, and compliance language must move with every synced lead.