Vendor Risk Assessment — LunchFlow

Vendor Risk Assessment: LunchFlow

Vendor Name: LunchFlow (lunchflow.app)

Service Provided: Consumer bank-account aggregation. The **user** holds the account and the contract; Orbiq reads that account on the user's behalf using an API key the user generates and pastes into Orbiq Core.

Assessment Date: August 16, 2026

Status: Approved (with mitigations) — **as a user-directed data source, not as an Orbiq processor.**

---

0. Why this assessment exists at all

The obvious argument for skipping it is that Orbiq has no relationship with LunchFlow: the user signs up, the user pays, the user can revoke. That argument is **rejected**, for three reasons, and the reasoning is recorded here because the ticket that commissioned this document allowed either outcome provided the decision was written down.

1. **Orbiq holds a live credential to the user's bank data.** The stored API key

is functionally a Plaid `access_token`. Whether Orbiq or the user pays the vendor has no bearing on what an attacker gets from Orbiq's database.

1. **Orbiq receives and retains the data.** Everything that arrives becomes

Tier 4 data under Orbiq's control, and Orbiq is the accountable organisation for it under PIPEDA 4.1.3 (RoPA §2.1).

1. **Orbiq advertises the path.** A capability marketed on the pricing page is a

capability Orbiq is answerable for, even when the commercial relationship sits elsewhere.

What this assessment explicitly does **not** do is certify LunchFlow's own processing. Orbiq has no contractual standing to audit them, no DPA to enforce, and no ability to compel disclosure. Sections 2 and 3 therefore separate **controls Orbiq operates** (verifiable, cited to code) from **facts about the vendor** (published by the vendor, unverified by us, and labelled as such).

---

1. Data Processing Context

- **Coverage:** wherever the user's own LunchFlow account reaches — advertised

by LunchFlow as 25,000+ institutions across 40+ countries via GoCardless (UK/EU), Akahu (NZ), Pluggy (BR), Finverse (parts of Asia) and MX / Finicity (North America). **No region gate in Orbiq**: a pasted key works wherever the vendor works, so Orbiq cannot bound this by geography the way the Plaid path is bounded.

- **Data category: Tier 4 / Restricted** — bank account metadata, balances,

transaction records, provider account identifiers, and the API key itself.

- **Direction:** LunchFlow → Orbiq (inbound read only). Orbiq never writes to

LunchFlow and never pushes user data to it beyond the authenticated GET.

- **Consent flow:** explicit and per-connection. The user must (a) create the

vendor account themselves, (b) authenticate each bank inside the vendor's own dashboard, (c) generate a REST API destination key, and (d) paste it into an authenticated Orbiq session. There is no path by which this happens incidentally.

- **Credential boundary:** bank credentials are entered at LunchFlow, never at

Orbiq. Orbiq holds only the derived API key.

- **Entitlement:** Orbiq Core (or trial). Gated behind the `lunchflow_enabled`

runtime flag, so the entire rail has a kill switch that does not require a deploy.

2. Technical Safeguards — controls Orbiq operates

These are verifiable in this repository.

- **Key storage:** the API key is Fernet-encrypted at the application layer

before persistence (`lunchflow_connections.api_key_enc`), under `PLAID_TOKEN_ENC_KEY` held in GCP Secret Manager. Never stored in plaintext, never written to logs, never returned to the client — including on the read path that renders the connection list.

- **Tenant isolation:** `lunchflow_connections` has RLS enabled with a policy

keyed to `app.current_owner_id`, mirroring `plaid_items`, with the `orbiq_system` escape reserved for the scheduler role (migration `c6f8a0d2e4b6`).

- **Encryption in transit:** TLS to the vendor API; the key travels only in an

`x-api-key` request header.

- **Least data:** Orbiq reads accounts, transactions, and balances. It does not

request, store, or display anything else the API happens to expose — notably, it does not read brokerage holdings for valuation, because Orbiq does not track live asset market values at all (domain rule: no phantom portfolios).

- **Blast-radius limit on failure:** an invalid or revoked key moves the

connection to `auth_error` and the scheduler stops polling it. There is a one-shot notification guard so a dead key cannot generate a notice every polling cycle.

- **Poll rate:** roughly every 6 hours (`LUNCHFLOW_SYNC_POLL_HOURS`), with

manual refresh under a daily allowance. Orbiq's outbound call volume is therefore bounded and predictable.

- **Deletion:** removing the connection deletes the encrypted key row.

Transactions already imported are retained deliberately — they are the user's ledger, not a cache of the vendor's data — and this is stated to the user rather than left to be discovered.

3. Vendor-published facts — **not verified by Orbiq

Recorded for completeness and explicitly flagged as unverified. Orbiq has no DPA, no audit right, and no SOC 2 / ISO 27001 report from this vendor, because Orbiq is not their customer. **Do not cite this section as assurance.**

- LunchFlow states that bank authentication occurs on its regulated upstream

rails and that it does not expose bank credentials to API consumers. Orbiq's observed behaviour is consistent with this (no credential field exists in the API surface Orbiq calls), but consistency is not verification.

- LunchFlow publishes its own pricing (from USD $5/mo for 4 accounts, +USD $1

per additional account) and its own terms. Orbiq restates these figures for the user's budgeting and does not warrant them; they are the vendor's to change without notice to us.

4. Residual Risk & Mitigations

Risk factor	Assessment	Orbiq mitigation	Residual
No DPA / no SCCs	Orbiq cannot contractually bind the vendor's handling, retention, or sub-processors	Informed per-connection consent; the arrangement is disclosed as third-party on every surface that mentions it (enforced by `scripts/claims_audit.py`); the user retains unilateral revocation at the vendor	**Accepted, disclosed.** Not equivalent to the Plaid path and never presented as such
API key compromise at Orbiq	Key grants read of the user's bank data	Fernet at rest, key in Secret Manager, never logged, RLS-scoped, decrypted in memory only at call time	Low
Vendor breach or shutdown	Orbiq has no visibility and no contractual notice right	Sync stops; already-imported transactions are unaffected and remain exportable; user re-pastes or abandons the rail with no data loss inside Orbiq	**Accepted** — the import-first architecture means loss of this rail degrades convenience, never the ledger
Unbounded geography	No region gate is possible on a pasted key	Not treated as a security control; the ledger is currency- and country-agnostic by design, so no code path assumes a region	Low
User confusion about who holds their data	The genuine risk of a BYO-key rail: a user may believe Orbiq vetted the vendor	ORBQ-525 rewrote every marketing surface to name the separate signup, the separate bill, and the third party *in the sentence making the claim*; this document states the non-vetting explicitly	**Primary residual risk. Monitor.**

Vendor price change	User's second bill can move without notice to Orbiq	Orbiq renders vendor pricing from server config, never a hardcoded literal, so a correction ships without a deploy	Low

5. Continuous Oversight Plan

- **Quarterly:** re-read LunchFlow's published terms and pricing; correct the

restated figures on the marketing surface within the same quarter if they have moved. Re-run `scripts/claims-audit.py`.

- **Continuous:** all outbound vendor calls are logged (metadata only, never the

key) for anomaly tracking; `lunchflow_enabled` is a live kill switch.

- **On event:** treat a suspected key compromise as a Tier 4 credential incident

under the Incident Response Playbook — delete the stored keys, notify affected users, and instruct them to rotate at the vendor. **Orbiq cannot revoke the key upstream; only the user can.** This asymmetry against the Plaid path (where `/item/remove` is available to us) is the reason this rail is documented separately.

- **Trigger for re-assessment:** any of — Orbiq entering a commercial

relationship with LunchFlow; the vendor requiring OAuth instead of a static key; a change that would let Orbiq write to the vendor; or the rail becoming the default rather than the opt-in path.

6. Related artifacts

- Record of Processing Activities — activity 08, controller determination §2.1
- Data Classification Policy — Tier 4, Aggregator Access Credentials
- Vendor Risk Assessment: Plaid — the contracted counterpart to this rail