Claims → evidence map

Bank-sync privacy claims → governing artifact

Effective Date: August 16, 2026
Document Status: Version 1.0 (Official)
Owner: Privacy Officer

Every claim Orbiq makes publicly about bank-sync privacy, mapped to the artifact that substantiates it. This exists so that publishing the governance set at `/trust` cannot create a documented inconsistency: if a claim on the live site has no row here, it has no substantiation, and per the workstream's first invariant it is deleted rather than softened.

Regenerate the evidence side of this table by reading the cited file. Do not edit a claim here without editing the page it quotes.

A. Claims Orbiq makes, and what backs them

#	Public claim (verbatim or near)	Where it appears	Governing artifact	Code / contract evidence
A1	"Bank linking is read-only. Orbiq Connect links through a regulated provider — your credentials never touch Orbiq."	homepage privacy band	VRA: Plaid §1, §2	Plaid Link is client-side; Orbiq exchanges a public token only. `routers/plaid.py`
A2	"no bank password ever reaches Orbiq" (LunchFlow path)	features, setup guide, FAQ	VRA: LunchFlow §1 credential boundary	Orbiq's client sends only `x-api-key`; no credential field exists in the API surface called. `services/lunchflow_client.py:135`
A3	"Orbiq only ever holds the key from your own LunchFlow account, and it's encrypted at rest"	setup guide	Data Classification Policy Tier 4 → Aggregator Access Credentials	`models/lunchflow_connection.py` — `api_key_enc`, Fernet under `PLAID_TOKEN_ENC_KEY`
A4	"never returned to your browser or written to logs"	setup guide	Data Classification Policy Tier 4 storage requirement	`models/lunchflow_connection.py` docstring; no serializer exposes `api_key_enc`
A5	"removing the connection stops the sync while leaving the transactions you've already imported untouched — they're your data"	setup guide	RoPA activity 08, retention column	Connection delete removes the key row; transactions are `Transaction` rows under ID 02 rules
A6	"Only merchant structure leaves the box… never your raw transaction rows"	homepage privacy band, FAQ	AI PIA; RoPA activity 03	`services/sanitizer.py` (PROFILE_FULL is the default for any new caller)
A7	"audit logs are PII-redacted"	homepage privacy band	Information Security Policy; RoPA activity 04	Redaction applied before the log stream

A8	"Natively, only Canada and the US" / native sync is CA-US only	homepage comparison + FAQ, features FAQ, pricing card	RoPA activity 07 (region gate); VRA: Plaid §1	`PLAID_REGION_CURRENCIES`; Connect-tier gate in `routers/plaid.py`
A9	"automatic sync in 40+ countries requires your own LunchFlow account… billed separately by LunchFlow and not included in this price"	pricing card, comparison, FAQ, features, three landing pages, llms.txt	RoPA §2.1 (disclosure obligations); VRA: LunchFlow §0, §4	Enforced continuously by `scripts/claims-audit.py`; test `backend/tests/test_claims_audit.py`
A10	"How many bank connections the free trial includes" (rendered, never hardcoded)	trial card	— (product claim, not privacy)	`services/billing.py:1426 trial_plaid_items`; grant-time ceiling `can_grant_trial_plaid_item` (`billing.py:819`); edge render `_middleware.ts composeHome`
A11	"data is encrypted at rest"	homepage privacy band	Data Classification Policy §4	Cloud SQL CMEK / AES-256 + RLS tenant isolation
A12	"download a full backup yourself any time (email-verified)"	homepage privacy band	Data Retention & Deletion Policy	`routers/backup.py:132` — `export_backup`, OTP-gated via `consume_backup_pass`

B. Claims Orbiq deliberately does not make

Recorded because their absence is a decision, and a future editor who "improves" the copy by adding one would be creating an unbacked claim.

Claim we could make but don't	Why not
"We have vetted LunchFlow's security."	No DPA, no audit right, no SOC 2 report — Orbiq is not their customer. VRA: LunchFlow §0 and §3 say this explicitly.
"LunchFlow is our processor."	It is not. Asserting it would claim a control Orbiq does not have. RoPA §2.1(2).
"Bank-grade security."	Puffery with no evidence row. Removed from `features.html` and `user-guide.html` in ORBQ-525; the mechanism is named instead.
"Your data is deleted when your trial ends."	The reaper archives rather than deletes (`services/trial_lifecycle.archive_user`) while its own notice emails say "deleted". Fix the mail before making any public retention promise. Noted in `index.html` at the pricing block.
"Works with any bank."	Replaced with the mechanism ("it reads the picture, not the bank") — an absolute is unverifiable.
Any aggregate rating or review count.	Zero real reviews. Never fabricate; noted in the JSON-LD comments on both `index.html` and `features.html`.

C. Gaps found during this mapping

Gap	Status
RoPA had no LunchFlow activity while the rail was live in production.	**Closed** — activity 08, this revision.

Data Classification Policy classified "Plaid Connection Data" by vendor name, leaving the LunchFlow key unclassified.	**Closed** — Tier 4 now classifies by capability, so the next rail is covered on the day its column is created.
No VRA existed for LunchFlow, and no written rationale for its absence.	**Closed** — `assessments/Vendor_Risk_Assessment_LunchFlow.md`.
The setup guide quoted an in-app label ("Global bank sync (LunchFlow)") that the app no longer uses.	**Closed** — guide now quotes "Global banks via LunchFlow" per `components/connect/LunchFlowSection.tsx:32`.
Trial-end retention wording contradicts the reaper's own notice emails.	**Open** — see row 4 of section B. Not a marketing fix; the email copy is the thing that is wrong.