Vendor Risk Assessment — Plaid

Vendor Risk Assessment: Plaid Inc.

Vendor Name: Plaid Inc.

Service Provided: Consumer-permissioned bank account aggregation (account metadata, balances, and transaction sync) for the Orbiq **Connect** tier.

Assessment Date: June 1, 2026

Status: Approved (with mitigations)

1. Data Processing Context

- **Coverage:** US & Canada only (Connect tier region gate).
- **Data Category: Restricted** — bank account metadata, balances, and transaction history retrieved on the user's behalf after explicit consent via **Plaid Link**.
- **Consent flow:** Plaid Link is surfaced **only to an authenticated Orbiq session** (Google OAuth, MFA enforced by Google) and only for **paid Connect** subscribers. Linking is an explicit, user-initiated action.
- **Direction:** Plaid → Orbiq (inbound). Orbiq does not push consumer data to Plaid beyond the public token exchange.

2. Technical Safeguards

- **Token storage:** Plaid `access_token`s are encrypted at the application layer with a **Fernet** key (`PLAID_TOKEN_ENC_KEY`, held in GCP Secret Manager) before persistence in Cloud SQL. Tokens are never logged.
- **Webhook integrity:** inbound Plaid webhooks are verified via **ES256 JWT** signature (JWKS from `/webhook_verification_key`), body SHA-256 binding, and a 5-minute freshness window; replays are blocked by request-id idempotency.
- **Encryption in transit:** TLS 1.2+ for all Plaid API calls.
- **Least data:** only `/transactions/sync` (cursor) is used for transaction retrieval; `/transactions/refresh` is never wired to any user control.
- **Certifications:** Plaid maintains SOC 2 Type II and ISO 27001; reviewed annually by the Privacy Officer.

3. Contractual & Regulatory Controls

- **DPA / SCCs:** Plaid's Data Processing Agreement and Standard Contractual Clauses govern the cross-border (Canada → US) transfer.
- **PIPEDA accountability:** Orbiq remains accountable under PIPEDA 4.1.3; consumer disclosure of US processing is provided at onboarding and in the Privacy Policy.

4. Residual Risk & Mitigations

Risk Factor	Assessment	Orbiq Mitigation
Cross-border (US) processing	Data leaves Canada; US CLOUD Act exposure	DPA + SCCs; consumer disclosure & consent; region gate to US/CA
Access-token compromise	Token enables read of bank data	Fernet encryption at rest, key in Secret Manager, never logged; revoke + `/item/remove` on incident
Webhook spoofing	Forged sync triggers	ES256 JWT verify + body hash + freshness + idempotency
Orphaned live items (cost + exposure)	Items for lapsed/non-entitled users	Automated reaper: `/item/remove` + token deletion on downgrade/lapse/idle

5. Continuous Oversight Plan

- **Annual:** review Plaid SOC 2 / ISO 27001 reports.
- **Continuous:** Axiom logging of all Plaid API calls for anomaly tracking; metered call counters + global kill switch.
- **On event:** Incident Response Playbook covers token compromise (revoke + reap).