CASE STUDY · BANKING & FINANCIAL SERVICES · DATA CONTROL & ENTERPRISE DATA BOUNDARY

A global bank proved its data never trained anyone else's model

Contractual assurance was not evidence. The Data Control Gateway verified training exclusion before every route and hashed the verification alongside the action.

Scenario	Published	Orcher components
Global bank · tier 1 · 38 jurisdictions	2026-09-02	Data Control Gateway, Immutable Audit Ledger, Observability

Summary

A tier-1 bank had training-exclusion clauses with four model providers and no way to demonstrate they had been honoured on any specific request. Orcher moved the guarantee from the contract into the execution path: no route completes unless the boundary is verified first, and the verification is part of the permanent record.

0
routes completed without a verified boundary check
across 1.4m directives

14% → 0%
of agent traffic bypassing the gateway

38
jurisdictions covered by one enforcement point

2 hours
to answer a regulator's per-request evidence demand
previously unanswerable

The situation

- Four model providers, each with a different training-exclusion posture, reached through six internal platforms with no common enforcement point.
- Regulators in three jurisdictions had asked, in writing, for evidence that customer data had not entered third-party training corpora. The bank could produce contracts, not evidence.
- An internal review found 14% of agent traffic bypassing the approved gateway entirely through direct SDK calls.

What Orcher enforced

- Data Control Gateway became the single egress for model traffic; direct SDK routes were revoked at the network and identity layer in the same change window.
- Every route now carries a pre-flight boundary check — provider, endpoint, contractual posture and data classification — and fails closed when any of the four disagree.
- Classification is enforced per directive rather than per application, so a single workflow can hold different boundaries for different data classes.
- The verification result is hashed into the Immutable Audit Ledger with the action, so evidence is produced as a by-product of execution rather than a project.

The data

Control	Contractual only	Enforced by Orcher
Training exclusion	Clause in MSA	Verified pre-route, per request
Evidence of exclusion	None	Hashed with the action
Coverage of agent traffic	86%	100%
Data class granularity	Per application	Per directive
Failure behaviour	Route proceeds	Fails closed, logged

The bank's own control-comparison table, reproduced with permission.

Outcomes

- Two jurisdictional regulators closed open information requests on the basis of the per-request evidence.
- The bank standardised on one enforcement point for all model traffic, retiring three partial internal proxies.
- New provider onboarding now takes days rather than a quarter, because the boundary control is provider-agnostic.
- Business units stopped negotiating their own model contracts — there was no longer an advantage to doing so.

> “A clause tells you what someone promised. We needed to show, request by request, what actually happened.”
>
> — Group Head of Data Risk, tier-1 global bank (composite, modelled scenario)

Read further

- The Data Control Gateway — dippai.com/research/vol-1-enterprise-superintelligence
- Trust and standards — dippai.com/trust
- Full case study — dippai.com/case-studies/global-bank-enterprise-data-boundary

Disclosure. Modelled reference scenario. The organisation is representative of the sector and scale described, not a named customer. Figures are produced by Orcher's own observability and ledger instrumentation for this configuration over the stated period and have not been independently audited. Market figures carry their own source line.