FA-02: Data Sovereignty Fragmentation

The Hidden Cost of Disconnected Customer Identities in Global Tourism

Page 1: The Diagnosis

KEY TAKEAWAY

> Systemic friction arises from the fragmentation of customer identity across disconnected functional silos. Without overarching data sovereignty, the customer remains "invisible" at the point of service, preventing real-time personalization and driving up the costs of service recovery.

Systemic Anatomy

The Symptom: Customer identity, preferences, and transaction history exist in disconnected functional databases (Sales CRM, Operations PMS, Loyalty) with no unified record accessible in real-time at service delivery.

The Root Cause: Data Governance Absence

Why It Recurs: Departments independently procure SaaS solutions optimized for their function without enterprise-level data integration requirements or enforcement.

The Governance Failure: No central Data Governance authority with power to mandate integration standards; customer data 'ownership' is politically contested across business units.

Scope Boundary: Does not explain data entry errors, inadequate data collection, or privacy/compliance issues unless directly caused by fragmentation across systems.

Page 2: Strategic Risk & Impact

STRUCTURAL RISK PROFILE

Blast Radius: cross-domain

Time to Impact: delayed

Reversibility: costly

Decision Frequency: medium

DECISION FALLOUT & IMPACT PATTERNS

Typical Decisions Affected:

- Allowing business units to select vendors without IT integration certification
- Operating separate databases for loyalty and operational delivery without synchronization

Delayed Effects:

- High-value customers are invisible during service recovery moments
- Personalization engines fire irrelevant offers based on incomplete profiles

Early Warning Signals:

- Staff asking customers for information already stored elsewhere in the company
- Different departments reporting conflicting metrics for the same customer action

INDUSTRY MANIFESTATIONS

Airlines:

- Difficulty escalating complex issues
- Confusing fare class differences

Hospitality & Hotels:

- Unclear about available services
- Poor recognition of loyal guests

Page 3: The AERIM Resolution

MOVING BEYOND LOCAL FIXES

Data Sovereignty Fragmentation is typically addressed through expensive MDM (Master Data Management) projects that attempt to create a single source of truth by syncing customer data across systems. These initiatives routinely fail because they treat fragmentation as a technical integration problem rather than a governance failure. AERIM resolves FA-02 through Sovereign Identity Nodes: instead of syncing data, each system retains ownership of its data but exposes it through a standardized protocol. A high-value customer's loyalty status remains in the CRM, their booking history in the PMS, but AERIM's Layer 3 (Decision Logic) can recognize and act on their complete profile across all touchpoints. This shifts the architecture from 'sync and replicate' to 'federate and query.'

Resolution Level Required: executive

This friction requires executive-level resolution because it involves adjudicating between competing business unit interests and imposing integration requirements that constrain departmental autonomy. Lower-level initiatives lack the organizational authority to mandate cross-functional data standards or override business unit procurement decisions.

TYPE OF CHANGE REQUIRED

Customer Data Ownership Clarification:

- Fragmentation is sustained by ambiguous ownership of customer records across organizational boundaries. The change required involves explicitly designating data stewardship responsibility and resolving political contests over customer relationship ownership.

Data Governance Authority Establishment:

- Data fragmentation persists because no organizational entity has cross-functional authority to mandate integration standards. The required change involves creating a governance structure with decision rights that supersede business unit autonomy in data architecture matters.

Procurement Authorization Redesign:

- Departmental tool proliferation continues when vendor selection authority resides entirely within business units. The friction recurs until procurement decisions above a certain threshold require certification of data integration compatibility as a mandatory approval criterion.

WHAT DOES NOT WORK

- MDM implementations fail when deployed without organizational mandate to enforce compliance. These projects address the symptom while leaving intact the business unit autonomy that created fragmentation

in the first place.

• Building individual connections between systems creates an unsustainable web of dependencies. This approach fails structurally because it treats fragmentation as a technical problem rather than a governance problem, and scales poorly as system count increases.

• Efforts to improve data quality within one functional area fail because the constraint is architectural, not operational. Cleaning data in isolation does not address the absence of synchronization mechanisms across systems.

CONCLUSION

Resolving FA-02 is an executive-level decision. It requires a mandate to transition from tool-centric procurement to an architecture-first approach. AERIM provides the structural foundation to address the root governance and coordination failures that perpetuate this friction archetype.