

PAYMENTS SIGNAL REFERENCE ARCHITECTURE

SYNTHETIC / TRAINING ONLY

Sanctions screening, list ingestion, matching, alert, investigation, tuning, and governance architecture

Trace how current sanctions data becomes a controlled screening decision, a reviewable alert, and evidence that tuning did not silently remove coverage.

Version: Payments Signal reference architecture v1

Reviewed: 2026-07-23

REFERENCE POSTURE

This architecture teaches the control chain from authoritative list through policy, matching, hold, investigation, decision, and assurance. It does not prescribe legal scope, list combinations, matching mathematics, threshold, auto-disposition, release authority, record retention, or reporting duties.

COMPONENTS

01 Official lists and regulatory obligations [external-network]

Owner: Sanctions authorities and compliance legal team

Provides authoritative sanctions designations, changes, identifiers, programmes, and legal context.

02 List ingestion, quality, and publishing hub [data-store]

Owner: Sanctions data management

Normalises authoritative records while retaining source lineage, effective time, identifiers, scripts, and change history.

03 Screening policy and field-coverage map [control]

Owner: Sanctions compliance governance

Defines who and what is screened, at which lifecycle points, from which message fields, under which jurisdictional and product rules.

04 Matching and screening engine [service]

Owner: Screening platform engineering

Compares normalised party, bank, geography, vessel, goods, and narrative data with the approved list snapshot and policy.

05 Payment hold and release gate [control]

Owner: Payment operations and sanctions control

Prevents the payment from advancing while an in-scope screening result is unresolved.

06 Alert queue and case service [application]

Owner: Sanctions operations

Creates one reviewable case with candidate, payment, party, list, policy, and matching evidence.

07 Investigation and disposition [operations]

Owner: Sanctions investigators and escalation teams

Compares reliable identifiers, ownership, context, and source evidence before recording a reasoned decision.

08 Tuning, testing, governance, and audit [operations]

Owner: Sanctions governance, quality assurance, model risk, and internal audit

Measures performance above and below thresholds, approves changes, samples decisions, and proves that coverage remains effective.

INTERFACES

- 01 Authoritative list update
 - sanctions-sources -> sanctions-list-hub | file | batch
- 02 Approved list snapshot
 - sanctions-list-hub -> sanctions-engine | file | batch
- 03 Policy and field map
 - sanctions-policy -> sanctions-engine | control | synchronous
- 04 Payment screening request
 - sanctions-payment-gate -> sanctions-engine | message | synchronous
- 05 Screening outcome
 - sanctions-engine -> sanctions-payment-gate | control | synchronous
- 06 Candidate alert
 - sanctions-engine -> sanctions-alerts | event | asynchronous
- 07 Investigation assignment
 - sanctions-alerts -> sanctions-investigation | operator | operator
- 08 Authorised disposition
 - sanctions-investigation -> sanctions-payment-gate | control | operator
- 09 Approved configuration change
 - sanctions-assurance -> sanctions-policy | control | operator
- 10 Outcome and performance evidence
 - sanctions-engine -> sanctions-assurance | event | asynchronous

TRACES AND STRESS CASES

TRACE: List update to payment release

1. Receive an official update - Source version received
2. Publish a complete snapshot - List snapshot approved
3. Apply approved scope - Policy version active
4. Hold and screen - Payment held for control
5. Create a candidate - Alert created
6. Record a reasoned disposition - Decision authorised
7. Apply the decision once - Released, rejected, blocked, or escalated

STRESS: List update is incomplete

Settlement: No settlement state changes because of the failed publication.

Funds: Payments follow the approved continuity posture.

Owner: Sanctions data management

Safe action: Do not publish the partial list; retain and disclose the last verified version.

STRESS: Screening engine is unavailable

Settlement: Settlement has not been authorised by this architecture.

Funds: Funds may remain reserved or unposted under product rules.

Owner: Payment and sanctions operations

Safe action: Use the approved fail-closed or formally documented continuity posture; never convert error to clear.

STRESS: Below-threshold test finds a true match

Settlement: Past settlement states vary and must be investigated.

Funds: Affected payments require trace and legal assessment; no blanket reversal is implied.

Owner: Sanctions compliance leadership

Safe action: Contain the configuration, identify the affected population, rescreen, investigate, and meet reporting duties.