

AIL/Core — Intake · Workflow · SLA · Audit · Compliance · Adjudication

Design Document (v1)

Date: November 05, 2025

Author: Prepared for: Heath (Software Architect)

1) Executive Summary

Build a mobile-first **intake and workflow core** for background screening that is:

- A **Subject-first system** (one person → one canonical record).
- An explicit **state machine** with visible **SLA** and **regulatory clocks** (no timers hidden in sagas).
- **Event-sourced** with **CQRS** read models for instant visibility and audit.
- **Compliance-by-construction** (FCRA/EEOC/613/611, Fair-Chance overlays, CA ICRAA) with immutable evidence packs.
- **Adjudication matrices** that are explainable, policy-as-data, and fair-chance aware.
- Integrations are **adapters** behind an anti-corruption layer (stubs in v1).

Non-goals (v1): deep provider automations, full pricing/billing engine, postal letters (email/SMS only).

2) Scope & Objectives

Primary objectives

- Sub-minute intake from invite → submit (P50), P90 < 24 hours.
- Queryable **SLA** and **pre-adverse/adverse** clocks; breach alerts.
- Immutable **audit ledger** and **Timeline** per Order/Subject.
- **Notifications** with policy-driven rules across email/SMS/webhooks.
- **Adjudication** decisions that are deterministic, explainable, and human-conferrable.
- **Policy snapshots**: configuration, not per-client forks in code.

Out-of-scope (v1): Full court/drug/MVR automation (use stubs), multi-region residency (design-ready, v2).

3) Architecture Overview

Flow:

ATS/HRIS/PM → **Intake API** → **Orchestrator** → **Provider Adapters (stubs)** → **Data Normalization** → **Adjudication** → **Adverse Action/Disputes** → **Reporting/Billing**

■ **Consent/IDV** ■ ■ **Ledger/Audit** ■

Principles

- **DDD** with bounded contexts; **CQRS + Event Sourcing**.
- **Events** are the source of truth; read models provide instant visibility.
- **PII minimization** & field-level encryption; immutable WORM artifacts.

4) Ubiquitous Language (DDD)

- **Subject** — Person being screened (canonical identity; dedup/merge capable).
 - **Order** — Screening request for a Subject under a package and policy snapshot.
 - **Product** — Unit of work (criminal, MVR, TWN); abstracted behind adapters.
 - **Consent** — Signed authorization/disclosure artifacts tied to an Order.
 - **Clock** — SLA or regulatory timer with business-day math and deadlines.
 - **Policy** — Versioned configuration (tenant/client/role/jurisdiction overlays).
 - **Notice** — Pre-adverse/final communications + delivery proofs.
 - **Timeline** — Ordered, immutable events for audit and UI.
 - **Assessment** — Adjudication evaluation and outcome for an Order.
-

5) Bounded Contexts

- 1) **Intake** — Invites, OTP verification, consents, PII, IDV (optional).
 - 2) **Order Workflow** — State machines, transitions, package routing (abstract).
 - 3) **SLA/Clocks** — Business calendars, deadlines, at-risk/breach detection.
 - 4) **Notifications** — Rules, channels (email/SMS/webhook), delivery proofs.
 - 5) **Compliance Policy** — FCRA/EEOC/613/611, Fair-Chance, ICRAA, DOT overlays, policy packs.
 - 6) **Adverse Action** — Two-step process, notices, evidence packs, disputes integration.
 - 7) **Adjudication** — RuleSets, Assessments, Charge Taxonomy, human-in-the-loop.
 - 8) **Subject Registry** — Canonical identity, aliases, merges, lineage.
 - 9) **Audit/Ledger** — Event store, WORM artifacts, projections.
 - 10) **Provider Adapters** — Anti-corruption layer; stubs for v1.
-

6) Aggregates & Invariants (selected)

Subject (Root)

- One canonical record per person. Aliases allowed; merges preserve lineage.
 - PII encrypted; SSN tokenized.
- Events:** Subject.Registered, Subject.AliasAdded, Subject.Merged.

Order (Root)

- States: created → invited → intake_in_progress → intake_complete → ready_for_routing → in_progress → ready_for_report → closed.
 - Must bind a Subject and a **policy_snapshot_id**.
- Events:** Order.Created, Invite.Sent, Consent.Captured, Intake.Submitted, Order.StateChanged, Order.Canceled.

Clock (Root; SLA & Adverse)

- Deterministic deadlines with business-day math; pausable; visible index.
- Events:** Clock.Started, Clock.AtRisk, Clock.Breached, Clock.Paused, Clock.Resumed, Clock.ReadyToAdvance.

Notice (Entity under Adverse)

- Template ids + render hashes; delivery proofs; artifacts in WORM.
- Events:** Notice.Prepared, Notice.Sent, Notice.DeliveryFailed, Notice.Delivered.

Assessment (Adjudication Root)

- States: prepared → recommended → under_review → finalized.
- Events:** Assessment.Prepared, Assessment.Recommended, Assessment.Override, Assessment.Finalized.
-

7) State Machines

Order

created → invited → intake_in_progress → intake_complete → ready_for_routing → in_progress → ready_for_report → closed

Guards: intake_complete requires Consent.Captured; ready_for_routing requires policy/subject bound.

Adverse Action

idle → pre_sent → [paused ↔ pre_sent] → ready_final → final_sent → closed

SLA clocks (examples)

- Intake SLA: invited → intake_complete ≤ X business hours.
- Routing SLA: intake_complete → ready_for_routing ≤ Y business hours.
- Overall SLA: created → ready_for_report ≤ Z days (read-only v1).

8) Policies as Data (versioned)

Snapshot the exact policy at Order creation; store its id forever.

```
id: pol_cli_acme_2025_11_01
intake:
  require_idv: true
  ssn_full: false
  address_years: 7
sla:
  intake_hours: 4
  routing_hours: 2
adverse:
  start_on: sent      # or delivered
  wait_business_days: 5
notifications:
  on_state:
    - when: order.invited
      channels: [email, sms]
      to: [subject]
      template: invite_v2
    - when: clock.at_risk
      channels: [email, webhook]
      to: [client_ops]
      template: sla_at_risk_v1
locales: { default: en-US }
branding: { logo_url: https://cdn/acme/logo.svg }
```

9) Clocks & Business-Day Math

A dedicated **BusinessCalendar** service provides:

- add_business_days(ts, n, jurisdictions[]) → deadline_ts
- diff_business_seconds(a, b, jurisdictions[]) → seconds

Clock Index (read model) — always queryable:

- adverse_action_clocks(clock_id, order_id, subject_id, client_id, state, pre_sent_at, deadline_at, remaining_business_s, pause_reason, jurisdictions, delivery_proofs_json, policy_snapshot_id, sla_status, created_at, updated_at)
- sla_clocks(clock_id, order_id, kind, state, started_at, deadline_at, sla_status, created_at, updated_at)

Watchdog flags on_track / at_risk / breached for dashboards & alerts.

10) Notifications

- Channels: email, SMS, webhook (postal in v2).
- Provider abstraction; every send emits Notification.Sent (with provider ids).
- Throttle/dedupe; retries with exponential backoff.
- Delivery failures trigger Notice.DeliveryFailed and can **pause** adverse clocks per policy.

11) Timeline & Audit

- **Event Store** (append-only) is canonical; outbox publishes to broker.
- **Timeline projection** composes domain events + artifact refs for applicant/client/ops views.
- **WORM Artifacts**: consents, notices, renders, signatures; events carry **hashes**, binaries stored with object-lock.
- **Export**: Evidence packs (zip of PDFs + JSON) per order/date-range for audits/subpoenas.

12) Compliance-by-Construction (Integrated)

Non-negotiable outcomes

- **Permissible Purpose (PP)** certification on every order.
- **Standalone FCRA disclosure + authorization** before screening; CA ICRAA overlays when applicable.
- **Two-step adverse action** with report copy + current CFPB Summary of Rights; visible, queryable clocks.
- **§607(b) Accuracy** & **§613 strict-procedures/notice** path for public records; record match fields.
- **§611 Disputes/Reinvestigation**: 30 days (+15 with new info); final adverse paused while open.
- **Seven-year reporting windows** for non-convictions; do not restart clocks.
- **Fair-Chance** (NYC/LA/SF/CA) gates + individualized assessment templates.
- **DOT Part 40** kept separate; MRO artifacts if enabled.
- **PBSA mapping** to speed accreditation audits.

Compliance Policy Packs (policy-as-data)

- **Federal Baseline**: FCRA/EEOC/CFPB forms; pre-adverse/final flows.
- **NYC FCA / LA County FCO / SF FCO**: post-offer sequencing + clocks + forms.
- **CA ICRAA**: extra disclosures and CA summary of rights.
- **DOT** (optional): MRO flow hooks; confidentiality.

Workflow Gates

- created → invited requires PP grant.
- intake_in_progress → intake_complete requires DisclosurePack acceptance.
- ready_for_report requires §613 strict-procedures pass or consumer notice proof.
- pre_adverse requires report + Summary of Rights artifacts attached.
- Criminal components blocked pre-offer in covered jurisdictions.

Evidence Packs (immutable)

- **Disclosure & Auth Pack** (FCRA + ICRAA as applicable).
- **§613 Pack** (strict-procedures calc or consumer notice).
- **Pre-Adverse Pack** (report, Summary of Rights, clock metadata).
- **Final Adverse Pack** (final letter, CRA contact, dispute info).

Compliance SLOs

- % orders with valid PP grant; disclosure defects; correct Summary-of-Rights version rate; 611 timeliness; Fair-Chance deadline adherence; §613 path usage.

13) Adjudication Matrices (Integrated)

Design Goals

- **Explainable** outcomes with reason codes & record lineage.
- **RuleSet as data** (versioned snapshots; deterministic).
- **Fair-Chance aware**; legal gates before evaluation.
- **Human-in-the-loop** overrides with justification & attachments.

RuleSet DSL (excerpt)

```
id: rs_cli_acme_finance_2025_11_01
defaults: { outcome: clear, lookback_years_default: 7, arrest_only_excluded: true }
criteria:
  - id: CRIT_FINANCIAL_FELONY_7Y
    when:
      any:
        - charge.category in [financial, theft_fraud]
          and disposition.verdict in [CONVICTED, PLED]
          and charge.severity == FELONY
          and time_since.most_relevant_years <= 7
    outcome: review
    reason_code: RC-FINANCIAL-LOOKBACK
```

Outputs include `recommended_outcome`, matched criteria, excluded records (and why), taxonomy & rule versions.

Charge Taxonomy

- Rule-based + curated statute map; versioned; curation queue for low-confidence mappings.

Events & Read Models

- RuleSet.Published, Assessment.Recommended, Assessment.Override, Assessment.Finalized.
- adjudication_queue, assessment_summary, matrix_impact_report projections.

Simulator & Analytics

- What-if simulations on historical normalized results; impact by role/jurisdiction; top ReasonCodes.

14) API Surface (OpenAPI sketches)

Orders & Intake

- POST /orders — create order
- POST /orders/{id}/invites — send magic-link (sms/email)
- POST /intake/sessions/{sid}/verify — OTP
- POST /intake/sessions/{sid}/consents — capture consent (artifact)
- POST /intake/sessions/{sid}/submit — finalize intake
- POST /orders/{id}/advance — controlled state transitions

Clocks & Timeline

- GET /clocks/adverse/{order_id} — visible regulatory clock
- GET /clocks/sla — query SLA clocks
- GET /timeline/{order_id} — auditable event stream

Compliance

- POST /compliance/permissible-purpose — certify PP
- GET/POST /compliance/policies — list/preview policy packs
- POST /compliance/613/check — strict-procedures vs notice evaluation
- POST /compliance/fair-chance/{order_id}/start — jurisdictional flow
- POST/PATCH /disputes — open/update disputes
- GET /evidence-packs/{order_id}/{type} — WORM bundle

Adjudication

- GET/POST /adjudication/rulesets — authoring & publish
- POST /adjudication/evaluate — run engine for an order

- POST /adjudication/assessments/{id}/override — human override
- POST /adjudication/assessments/{id}/finalize — freeze outcome

Webhooks we send

- order.created, invite.sent, intake.submitted, order.ready_for_routing
- clock.at_risk, clock.breached, pre_adverse.sent, final_adverse.sent
- notice.delivery_failed, assessment.recommended, assessment.finalized

15) Data Model (storage sketch)

Write (per context)

- subjects, subject_aliases, subject_links
- orders, order_policy_snapshots
- consents (render_hash, doc_version, signed_at, artifact_ref)
- clocks (aggregate snapshots) + events_outbox (idempotent)
- rulesets, assessments, assessment_matches
- compliance: pp_grants, disclosure_acceptances, fair_chance_clocks, section613_controls

Read

- order_summary, order_timeline_events
- adverse_action_clocks, sla_clocks
- adjudication_queue, assessment_summary
- notifications_history

Artifacts (WORM)

- /artifacts/{order_id}/{type}/{hash}

SQL Starters (excerpt)

```
create table events_outbox(  
    id uuid primary key, aggregate_id text, aggregate_type text,  
    event_type text, payload jsonb, occurred_at timestamptz default now(), published boolean default false  
)  
create table adverse_action_clocks(  
    clock_id uuid primary key, order_id text, subject_id text, client_id text,  
    state text, pre_sent_at timestamptz, deadline_at timestamptz,  
    remaining_business_s bigint, pause_reason text, jurisdictions jsonb,  
    delivery_proofs jsonb, policy_snapshot_id text, sla_status text,  
    created_at timestamptz default now(), updated_at timestamptz default now()  
)
```

16) Security & Privacy

- Field-level **AEAD encryption** for PII; SSN tokenization; least-privilege RBAC/ABAC.
- **PII minimization** in read models; artifact hashes in events (not raw).
- Object-lock (WORM) for evidence bundles; tamper-evident logs.
- Secrets vaulted; rotation policy; environment isolation.

17) Observability

- **Metrics**: invite→submit, intake P50/P90, on_track/at_risk/breached counts, notification send/fail, §611 dispute cycle time, assessment distribution.
- **Tracing**: command→events→projections (OpenTelemetry).

- **Dashboards**: At-Risk Clocks, Breaches by Client, Intake Funnel, Assessment Queue.
- **Alerts**: SLA breaches, adverse-action deadline proximity, notification failure spikes.

18) Technology Baseline (swappable)

- Language: TypeScript (NestJS) or .NET 8.
- Broker: Kafka (or SQS/SNS).
- DB: Postgres (write/read models); Object storage for artifacts; OpenSearch (later) for subject dedupe.
- Infra: Kubernetes + sealed secrets (or serverless path).

19) Provider Adapters (v1 stubs)

- Every product call is an idempotent job with a stable request/response contract.
- Publish Product.Requested → Product.Completed (fixture payloads).
- Anti-corruption layer isolates upstream from vendor-specific semantics.

20) Testing Strategy

- **State machine** property tests: illegal transitions rejected.
- **Clock math**: holidays; pause/resume; recompute; at-risk → breached.
- **Compliance**: Disclosure correctness, Summary-of-Rights versioning, §613 strict-procedures vs notice, §611 timelines, Fair-Chance gates.
- **Adjudication**: determinism; exclusions (arrest-only, stale non-convictions); rule/jurisdiction overrides; human override requirements.
- **Idempotency/chaos**: duplicate events, out-of-order deliveries, retries.

21) Delivery Plan (high-level milestones)

Phase 1 (Weeks 0–4): Foundations

- Aggregates: Subject, Order, SLAClock, AdverseActionClock.
- Outbox + broker + projections: order_summary, order_timeline, clocks.
- PWA intake MVP (invite→consent→PII→submit).
- Notifications (email/SMS) + rules v1; BusinessCalendar v1 (US + CA + NYC).

Phase 2 (Weeks 5–8): Compliance & Visibility

- Pre-adverse/final flows + evidence packs (email channel).
- Ops dashboard (at-risk/breached, resend invites, pause/resume clocks).
- Policy snapshots + tenant branding/locale.
- Adjudication engine v1 + queue + overrides (no simulator yet).

Phase 3 (Weeks 9–12): Adjudication & Hardening

- Charge Taxonomy curation; What-if Simulator; Matrix Impact Report.
- Webhooks for clients; audit export; SLO tracking; perf pass.

Phase 4 (Weeks 13–16): Pilot & Iterate

- Pilot with 1–2 CRAs; refine policies; add postal (optional) and IDV adapters.
- Prepare PBSA mapping dashboard for sales.

22) Marketability (review notes)

Category: Screening intake & workflow orchestration with compliance and explainable adjudication.

ICP: Mid-market CRAs and high-volume in-house screeners on legacy OS stacks.

Differentiators: Visible **Clock Index** and **Timeline**; policy snapshots (no code forks); evidence packs; deterministic adjudication + simulator.

Pricing idea: Platform fee + usage (orders) + “Compliance Pack” add-on.

Positioning: “Provable compliance and explainable decisions, without ripping out your CRA OS.”

23) Appendices (selected)

A. Event Contracts (excerpt)

- Order.Created, Invite.Sent, Consent.Captured, Intake.Submitted, Order.StateChanged, Clock.Started, Clock.AtRisk, Clock.Breached, Notice.Sent, Assessment.Recommended, Assessment.Finalized.

B. Example Requests (excerpt)

```
{ "cmd": "CreateOrder", "order_id": "ord_01", "client_id": "cli_01",
  "subject_ref": { "seed": { "first_name": "Avery", "last_name": "Nguyen", "dob": "1993-07-04", "ssn_last4": "1234" } },
  "package": "EMP_STD_US", "policy_id": "pol_cli_acme_2025_11_01" }

{ "evt": "Clock.Started", "clock_id": "clk_01", "kind": "adverse", "order_id": "ord_01", "deadline_at": "2025-11-12T12:00:00Z" }
```