Build a fraud and transaction-monitoring stack

A combined fraud and financial-crime architecture spanning device intelligence, identity, payment fraud, transaction monitoring, screening and cases.

LAYER 1 / REQUIRED

Device and behavioural signals

Detect account creation, takeover and anomalous behaviour.

- ☐ Signal coverage
- ☐ Latency
- ☐ Privacy and data quality

SEON — Device and digital-footprint intelligence
Sardine — Device and behavioural risk
Featurespace — Behavioural analytics

LAYER 2 / REQUIRED

Identity and account risk

Combine KYC decisions with fraud and account controls.

- ☐ Identity graph
- ☐ Synthetic identity controls
- ☐ Decision orchestration

Alloy — Identity decisioning
Persona — Identity workflows
Sumsub — Identity and fraud controls

LAYER 3 / REQUIRED

Payment fraud

Score authorisations, transfers or payouts.

- ☐ Transaction types
- ☐ Real-time latency
- ☐ Consortium and feedback data

Feedzai — Payment fraud
Featurespace — Fraud detection
Provenir — Risk decisioning

LAYER 4 / REQUIRED

AML monitoring and screening

Detect suspicious activity and restricted parties.

- ☐ Scenario and model coverage
- ☐ Screening data
- ☐ Alert quality

Hawk AI — Transaction monitoring
Unit21 — Monitoring and cases
ComplyAdvantage — Screening and monitoring
Napier AI — AML platform

LAYER 5 / REQUIRED

Cases and investigations

Investigate, document and escalate alerts.

- ☐ Workflow and audit trail
- ☐ Entity linking
- ☐ Regulatory reporting support

Unit21 — Case management
Quantexa — Entity and network analytics
Salv — Monitoring and collaboration

Questions to ask providers

- ☐ Which legal entity contracts for each service and in which jurisdictions?
- ☐ Which responsibilities remain with the product operator rather than the provider?
- ☐ What are the implementation, approval, testing and migration timelines?
- ☐ How are incidents, exits, data portability and business continuity handled?
- ☐ Which system is the decision authority when vendor scores conflict?