Build a KYC and AML stack

A layered customer-lifecycle control stack covering identity, business verification, screening, transaction monitoring, fraud, cases and crypto-specific controls.

LAYER 1 / REQUIRED

Identity verification

Verify individuals, documents and biometrics.

- ☐ Document and country coverage
- ☐ Liveness and fraud controls
- ☐ Manual review

Veriff — Identity and biometric verification
Jumio — Identity verification
Entrust Identity Verification — Identity and onboarding
IDnow — Identity verification and signatures

LAYER 2 / REQUIRED

Business verification and UBO

Verify companies, registries and beneficial owners.

- ☐ Registry coverage
- ☐ UBO resolution
- ☐ Complex ownership support

Trulioo — Global KYB
Sumsub — KYB and onboarding
Fenergo — Client lifecycle management
Persona — Configurable KYB workflows

LAYER 3 / REQUIRED

Sanctions, PEP and adverse media

Screen customers and counterparties against risk data.

- ☐ Data provenance
- ☐ Matching and transliteration
- ☐ Ongoing screening

ComplyAdvantage — Screening and risk data
LexisNexis Risk Solutions — Risk and identity data
Dow Jones Risk & Compliance — Sanctions, PEP and adverse media
Moody's — Entity and risk data

LAYER 4 / REQUIRED

Transaction monitoring and cases

Detect unusual behaviour and manage investigations.

- ☐ Rule and model configurability
- ☐ Case workflow
- ☐ Audit and regulatory reporting

Hawk AI — Transaction monitoring
Napier AI — Monitoring and screening
Unit21 — Monitoring and cases
Flagright — Monitoring and fraud

LAYER 5 / OPTIONAL

Fraud intelligence

Add device, behavioural and payment-risk signals.

- ☐ Signal coverage
- ☐ Latency
- ☐ Explainability and review tooling

SEON — Device and digital-footprint risk
Sardine — Fraud and AML
Feedzai — Fraud and financial crime
Featurespace — Behavioural fraud

LAYER 6 / OPTIONAL

Blockchain analytics and Travel Rule

Add onchain screening and counterparty information where digital assets are in scope.

- ☐ Chain coverage
- ☐ Risk methodology
- ☐ Travel Rule interoperability

Chainalysis — Blockchain analytics
TRM Labs — Blockchain intelligence
Elliptic — Crypto AML
Notabene — Travel Rule

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?
- ☐ How will false positives be measured and tuned?

- ☐ Which alerts require human review and who makes the final decision?