# AI for Financial Crime & AML Teams

A practical session for the teams stopping financial crime — using AI to find more, with the controls to defend every decision.

| WHO IT'S FOR | FORMAT | LENGTH |
| --- | --- | --- |
| Financial-crime, AML/CFT, fraud and investigations teams in banks and digital-asset firms. | In-house workshop | Half-day or full-day |

## What your team walks away with

Put AI to work on detection and investigations safely — knowing where it sharpens your team and where it quietly fails.

## What you'll learn

- ✓ Tell where AI genuinely improves detection and investigations from where it overpromises
- ✓ Cut false positives in alerts without missing the real risk, and prove the trade-off was sound
- ✓ Use AI to speed up investigations and case write-ups while keeping the analyst accountable
- ✓ Spot how criminals turn AI against you through synthetic identities, deepfakes and automated fraud
- ✓ Know where keeping a human in the loop is not optional, including suspicious-activity reporting
- ✓ Apply a financial-crime AI playbook of do's, don'ts and red flags in your own team

## Curriculum

### 01 Where AI genuinely improves detection and investigations

- The detection and investigation tasks where AI adds real value
- How AI-assisted monitoring differs from traditional rules and scenarios
- Areas where AI overpromises and shouldn't replace existing controls
- Matching AI tools to the typologies your team actually faces
- Setting realistic expectations before deploying anything

### 02 AI-driven alerts: cutting false positives without missing real risk

- Why traditional alerting produces so much noise
- How AI can triage and prioritise alerts more intelligently
- Tuning so fewer false positives doesn't mean more missed risk
- Tracking which alerts convert to reports to measure effectiveness
- Evidencing that the precision-versus-coverage trade-off was sound

### 03 Using AI to speed up investigations and case write-ups

- Where AI can accelerate research, summarisation and case narratives
- Drafting write-ups with AI while the analyst owns the conclusion
- Guarding against confident but wrong AI-generated summaries
- Keeping a clear evidence trail behind every AI-assisted step
- Quality checks before anything reaches a decision or a report

### 04 How criminals use AI against you — and how to spot it

- Synthetic identities and AI-generated documents in onboarding fraud
- Deepfake voice and video used in social engineering and authorisation fraud
- Automated and scaled fraud and laundering schemes
- Red flags that suggest an AI-assisted attack
- How detection has to adapt as attackers' tools improve

## 05 Keeping a human in the loop where it legally matters

- Decisions a person must own, not the model
- Why supervisors reject 'the AI said so' as a reason for a decision
- Human oversight in customer decisions and suspicious-activity reporting
- Designing review points so accountability stays with people
- Documenting human judgement alongside AI output

## 06 A playbook your team can adopt this quarter

- A practical playbook of do's, don'ts and red flags
- Clear rules for when to rely on AI and when not to
- Standard checks before acting on AI output
- Tailoring the playbook to bank or digital-asset operations
- Embedding it into existing investigation and reporting workflows

## You keep

> An AI-for-financial-crime playbook with do’s, don’ts and red flags.