JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

AI in Fraud Detection and Transaction Monitoring Course

25 – 29 April 2027
Kuala Lumpur

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

AI in Fraud Detection and Transaction Monitoring Course

Ref: 39_986 **Date:** 25 – 29 April 2027 **Location:** Kuala Lumpur **Fees:** 4900 GBP

AI in Fraud Detection and Transaction Monitoring is a 1-week training course for fraud analysts, internal auditors and risk and compliance officers, who leave with a fraud detection model blueprint carrying alert triage rules. Instant payments let fraudsters move money in seconds, while rule-based monitoring floods teams with mostly false alerts. Jupiter Prime Training runs this course on AI in fraud detection and transaction monitoring for those who stop losses and evidence controls.

Why AI in Fraud Detection and Transaction Monitoring Matters Now

Three forces shape AI in fraud detection and transaction monitoring today: real-time payments that shrink the window for intervention, organised fraud rings that spread activity across many accounts, and supervisors and boards who expect monitoring to be explainable and tested. Organisations that apply machine learning with discipline catch more genuine fraud with fewer customer interruptions; those that bolt models onto weak data see drifting scores and alert queues no investigator can clear. Examples come from card payments in retail banking and claims fraud in insurance. Model risk is treated with ISO/IEC 42001 for AI management systems and the NIST AI Risk Management Framework AI RMF.

Who Gains Most from AI in Fraud Detection and Transaction Monitoring

- Fraud analysts who investigate alerts, cases and loss events
- Transaction monitoring leads who tune scenarios, thresholds and queues
- Internal auditors who test the design and effectiveness of fraud controls
- Risk and compliance officers accountable for monitoring coverage and reporting
- Model validation specialists who challenge detection models before and after release

The strongest gain comes when a fraud analyst, a monitoring lead and an auditor covering the same payment channel attend together.

AI in Fraud Detection and Transaction Monitoring Capabilities

Participants learn to combine rules, anomaly scores and network signals into detection that auditors can test.

- Assess fraud typologies and data signals for each payment or claims channel — fraud strategy owners
- Apply anomaly detection and supervised scoring to transaction streams — monitoring leads
- Build network views that expose mule accounts and fraud rings — investigation managers
- Calculate false positive cost and detection rate trade-offs for thresholds — risk committees
-

Test models for drift, bias and explainability before and after release — model validation and audit
- Design a fraud detection model blueprint with alert triage rules — the head of financial crime

Key AI in Fraud Detection and Transaction Monitoring Terms

- Anomaly Detection — methods that flag transactions or behaviour that differ sharply from an established normal pattern.
- Transaction Monitoring — automated screening of payments and account activity to identify suspicious or fraudulent behaviour.
- Fraud Ring — a coordinated group using linked accounts, devices or identities to commit fraud at scale.
- False Positive — an alert raised on legitimate activity, consuming investigator time and disturbing customers.
- Model Drift — a decline in model accuracy as fraud tactics, customers or data change over time.
- Alert Triage — ranking and routing alerts so investigators handle the highest-risk cases first.

AI in Fraud Detection and Transaction Monitoring Day by Day

Day 1: Fraud Typologies and Monitoring Foundations

- Fraud Typology Mapping by Channel — Cards, Transfers, Claims and Onboarding
- Rule-Based Scenario Review — Strengths, Gaps and Alert Volumes
- Data Sources for Detection — Transactions, Devices, Sessions and Customer Profiles
- Loss and Alert Baselines — Measuring Current Control Performance
- AI Opportunity Assessment — Where Models Outperform Static Rules

Day 2: Anomaly Detection and Scoring Models

- Unsupervised Anomaly Detection — Isolation Forests and Clustering Choices
- Supervised Fraud Scoring — Label Quality and Class Imbalance
- Behavioural Profiling and Velocity Features — Signals of Account Takeover
- Real-Time Versus Batch Scoring — Latency and Intervention Points
- Hybrid Rules and Model Strategies — Combining Expert Logic With Scores

Day 3: Network Analysis of Fraud Rings

- Graph Construction From Shared Attributes — Accounts, Devices and Addresses
- Community Detection Methods — Exposing Coordinated Fraud Rings
- Money Mule Identification — Flow Patterns and Link Strength
- Entity Resolution Across Systems — Matching Identities Reliably
- Network Visualisation for Investigators — Case Building and Evidence

Day 4: False Positives, Drift and Model Risk

- Threshold Setting With Cost Curves — Detection Versus Customer Friction
- Alert Triage and Prioritisation Models — Investigator Capacity Decisions
- Drift Monitoring and Retraining Triggers — Adapting to New Tactics
- Explainability for Investigators and Auditors — Reason Codes and Evidence
- ISO/IEC 42001 and NIST AI RMF Controls — Fraud Model Risk

Day 5: Practising the Fraud Detection Model Blueprint

- Channel Typology and Data Profile — Applying Typology Mapping
- Scoring and Network Detection Design — Applying Anomaly and Graph Methods
- Threshold and Triage Rules — Applying Cost Curves and Prioritisation
- Validation, Monitoring and Audit Trail — Drift and Explainability Checks
- Fraud Detection Model Blueprint — Presentation to Financial Crime Leadership

Applying AI in Fraud Detection and Transaction Monitoring After the Course

- Measure the false positive rate of one monitoring scenario and model the effect of a revised threshold
- Build a link graph of accounts sharing devices and review the largest cluster with investigators

AI in Fraud Detection and Transaction Monitoring Questions FAQ

What is AI in fraud detection and transaction monitoring and why does it matter now?

AI in fraud detection and transaction monitoring uses anomaly detection, scoring models and network analysis to find fraud in payments and claims. It matters now because real-time channels and organised rings outpace static rules and overwhelm teams with false alerts.

Which roles gain most from AI in fraud detection and transaction monitoring training?

Fraud analysts, monitoring leads, internal auditors and compliance officers gain most. They design, tune, investigate and test detection controls and need to judge model outputs with confidence.

How does AI in fraud detection and transaction monitoring training differ from a general anti-fraud course?

It focuses on the models behind detection rather than fraud law or investigation interviews. You work on anomaly scoring, graph analysis, thresholds, drift and explainability so that monitoring decisions rest on tested evidence.

What do you bring back from AI in fraud detection and transaction monitoring training?

You bring back a fraud detection model blueprint for one channel. It sets typologies, data signals, scoring and network methods, thresholds, alert triage rules and the validation and monitoring checks auditors will review.

AI in Fraud Detection and Transaction Monitoring: The Way Forward

The fraud detection model blueprint first informs which channel moves from static rules to scored and network-based detection, and which triage rules investigators follow. Fraud, monitoring and audit leads use it to agree thresholds and validation evidence. After the first quarter of live alerts, revisit drift and false positive measures, since fraudsters adapt quickly once detection changes.