JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

AI-Driven Fraud Detection in Banking Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

AI-Driven Fraud Detection in Banking Training Course

AI-Driven Fraud Detection in Banking is a 1-week training course for bank fraud managers and financial crime analysts who need to leave with a Fraud Alert Tuning Playbook covering card, payment and account takeover threats. Instant payments and socially engineered scams now move money in seconds, so rule engines alone leave losses and customer friction rising together. Jupiter Prime Training frames AI-driven fraud detection in banking around those losses and that friction.

Why AI-Driven Fraud Detection in Banking Matters Now

Three forces reshape bank fraud desks: real-time payment rails that remove the window for manual checks, organised mule networks that recycle stolen funds across dozens of accounts, and customers who abandon a bank after repeated false declines. Machine learning scores catch patterns static rules miss, yet a poorly tuned model floods investigators with alerts or quietly drifts as fraudsters adapt. Sound oversight draws on ISO/IEC 42001 artificial intelligence management system and the NIST AI Risk Management Framework NIST AI RMF for validation, monitoring and accountability of scoring models.

Who Gains Most from AI-Driven Fraud Detection in Banking

- Leads who set fraud strategy and own the balance between losses and customer declines
- Analysts who investigate card, wire and instant payment alerts and feed outcomes back to models
- Specialists who trace mule account networks and coordinate account closures
- Practitioners who tune scoring thresholds and rule overlays for each payment channel
- Reviewers who validate fraud models and report drift to risk committees

Fraud operations units that send an investigator, a strategy lead and a model owner together gain most.

AI-Driven Fraud Detection in Banking Capabilities

Participants set, test and defend the scoring choices that decide which payments stop.

- Design channel-specific scoring strategies for card, transfer and login events — head of fraud
- Calculate alert economics from loss avoided, investigator hours and customer friction — finance and operations
- Apply graph analytics to expose mule rings and shared device clusters — financial crime investigators
- Test threshold changes with champion-challenger trials before release — model risk reviewers
- Build drift and feedback-loop monitoring for live fraud models — model owners

- Communicate false positive trade-offs in plain terms — customer experience leaders and executives

Key AI-Driven Fraud Detection in Banking Terms

- Account takeover — fraud in which a criminal gains control of a genuine customer's login or device to move funds.
- Authorised push payment scam — a fraud where the customer is tricked into sending money to an account the criminal controls.
- Money mule — a person or account that receives and passes on stolen funds to obscure their origin.
- False positive rate — the share of genuine transactions or logins wrongly flagged as fraudulent by a scoring model.
- Behavioural biometrics — signals such as typing rhythm or swipe pressure used to judge whether the real customer is present.
- Champion-challenger test — running a new scoring model beside the live one on real traffic to compare outcomes before switching.

AI-Driven Fraud Detection in Banking Day by Day

Day 1: Fraud Typologies and Payment Rail Pressures

- Card-Not-Present and Counterfeit Patterns — Where Card Losses Concentrate
- Instant Payment Scam Typologies — Why Manual Holds No Longer Work
- Account Takeover Journeys — Mapping Login, Device and Payee Changes
- Rule Engine Limits — Deciding Where Machine Learning Adds Detection
- Alert Economics Baseline — Pricing Losses, Investigator Time and Declines

Day 2: Scoring Models and Anomaly Detection

- Supervised Gradient-Boosted Classifiers — Scoring Labelled Card Transactions
- Isolation Forest and Autoencoder Methods — Surfacing Novel Payment Anomalies
- Feature Engineering From Velocity and Geolocation — Sharpening Risk Signals
- Behavioural Biometrics and Device Fingerprinting — Confirming Genuine Customer Presence
- Label Delay and Chargeback Feedback — Keeping Training Sets Honest

Day 3: Network Analytics for Mule Rings

- Entity Resolution Across Accounts and Devices — Linking Hidden Identities
- Graph Centrality and Community Detection — Exposing Mule Network Hubs
- Beneficiary Risk Scoring — Flagging Payees Before Funds Leave
- Cross-Channel Case Linking — Uniting Card, Wire and Login Evidence
- Explainable Reason Codes — Giving Investigators Defensible Alert Context

Day 4: Alert Tuning and Model Oversight

- Threshold Setting by Segment — Trading Detection Against Customer Friction
- Champion-Challenger Trials — Proving Gains Before Production Release
- Population Stability and Drift Indicators — Triggering Model Retraining
- ISO/IEC 42001 and NIST AI RMF Mapping — Evidencing Scoring Model Controls
- Bias and Fair Treatment Checks — Protecting Vulnerable Customer Groups

Day 5: Practising the Fraud Alert Tuning Playbook

- Live Alert Queue Simulation — Applying Scores and Reason Codes
- Mule Ring Investigation Exercise — Applying Graph Analytics to Case Data
- False Positive Reduction Sprint — Applying Segment Thresholds to Declines
- Risk Committee Briefing Rehearsal — Defending Drift and Retraining Choices
- Fraud Alert Tuning Playbook Completion — Assembling Thresholds, Monitors and Escalations

Applying AI-Driven Fraud Detection in Banking After the Course

- Recalculate alert economics for one payment channel and propose a revised score threshold backed by champion-challenger evidence.
- Run a graph query over recent scam beneficiaries to identify a suspected mule cluster for investigation.

AI-Driven Fraud Detection in Banking Questions FAQ

What is AI-driven fraud detection in banking, and why does it matter now?

It is the use of machine learning scores, anomaly detection and graph analytics to stop card, payment and account takeover fraud. It matters now because instant payments and scams move funds faster than manual checks can react.

Which roles gain most from AI-driven fraud detection in banking?

Fraud strategy leads, financial crime analysts and fraud model owners gain most, since each controls part of the chain from score to investigation outcome.

How does AI-driven fraud detection in banking differ from an anti-money laundering course?

It concentrates on stopping fraudulent payments and logins in real time and tuning the alerts behind them. An anti-money laundering course focuses on customer due diligence, suspicious activity reporting and the laundering lifecycle.

What do you bring back from AI-driven fraud detection in banking?

You bring back segment thresholds, a drift monitoring routine, a graph method for mule rings and a way to price false positives against losses.

AI-Driven Fraud Detection in Banking: The Way Forward

The Fraud Alert Tuning Playbook sets out score thresholds, reason codes, drift monitors and escalation routes for each channel. Its first use is usually a threshold change on the noisiest alert queue. Fraud leads and model owners work from it, and after release the decline-to-loss balance deserves a fresh look.