



Advanced Fraud Analytics and Data Mining Training Course

1 – 12 March 2027
Cairo



Advanced Fraud Analytics and Data Mining Training Course

Ref: 815_161726 **Date:** 1 – 12 March 2027 **Location:** Cairo **Fees:** 7000 Euro

Overview

Advanced Fraud Analytics and Data Mining Training Course is a two-week advanced course for fraud, risk, audit, compliance, and analytics professionals who leave with a Fraud Analytics Mining Playbook. Participants apply fraud analytics data mining, suspicious pattern detection, anomaly detection, fraud network analysis, and alert triage to convert fragmented signals into governed investigative decisions. The course connects model evidence, operational controls, and investigation handoffs. Agile Leaders Training Center develops advanced fraud analytics capability.

Who Should Attend

- Fraud analysis functions responsible for detecting and validating suspicious transaction and entity behavior
- Financial crime investigation functions responsible for turning analytical alerts into documented case leads
- Risk analytics functions responsible for building, evaluating, and monitoring fraud indicators
- Internal audit functions responsible for testing fraud risks, controls, and anomalous activity
- Compliance data functions responsible for controlled alert review and evidence handoffs
- Data specialists responsible for preparing features, labels, networks, and validation samples

The course assumes participants can analyze structured data, interpret model outputs, and document fraud-risk decisions, and leaves out introductory statistics, production software engineering, cybersecurity response, and legal certification preparation.

Departments and Industries

The course supports departments and industries that use analytical evidence to identify, prioritize, and investigate possible fraud.

- Fraud management, financial crime, compliance, internal audit, and enterprise risk departments
- Banking, payments, insurance, lending, and financial technology operations
- Retail, e-commerce, telecommunications, and digital-platform businesses
- Procurement, supply chain, manufacturing, and asset-intensive operations
- Healthcare claims, public services, and professional-service organizations

Learning Objectives

By the end of this course, participants will be able to:



- Apply fraud-risk hypotheses to analytical test design
- Build governed features, labels, samples, and network data
- Compare supervised, unsupervised, anomaly, and graph methods
- Evaluate imbalanced models, thresholds, explanations, and alert utility
- Prioritize alerts and build controlled investigation handoffs
- Build a monitored Fraud Analytics Mining Playbook

Course Agenda

Day 1: Frame Fraud Analytics Decisions

- Fraud Risk Hypothesis Canvas
- Fraud Scheme and Red-Flag Taxonomy
- Analytical Use-Case Prioritization Matrix
- Decision Owner and Stakeholder Map
- Fraud Analytics Control Boundary

Day 2: Prepare Governed Fraud Data

- Transaction and Entity Data Inventory
- Data Lineage and Permitted-Use Record
- Missingness and Data Quality Profile
- Identity Resolution and Entity Matching Rules
- Fraud Data Leakage Review Checklist

Day 3: Engineer Fraud Signals

- Behavioral Velocity Feature Catalogue
- Peer-Group Deviation Feature Set
- Temporal Sequence and Event Window Design
- Label Definition and Case Outcome Register
- Training, Validation, and Holdout Sample Plan

Day 4: Build Supervised Detection Models

- Logistic Regression Fraud Scorecard
- Decision Tree and Random Forest Comparison
- Gradient-Boosting Classification Workflow
- Cost-Sensitive Learning Decision Table
- Probability Calibration and Score Mapping



Day 5: Detect Unknown Fraud Patterns

- Statistical Outlier Baseline Profile
- Isolation Forest Anomaly Detection Method
- Clustering-Based Peer Segmentation
- Density and Distance Threshold Review
- Novel Pattern Investigation Queue

Day 6: Analyze Fraud Networks

- Entity-Relationship Graph Data Model
- Shared-Identifier Link Analysis
- Connected-Component Detection Method
- Community and Cycle Pattern Analysis
- Centrality and Suspicious Hub Scorecard

Day 7: Evaluate Detection Performance

- Class-Imbalance Evaluation Framework
- Precision, Recall, and Ranking Evidence Table
- False-Positive Cost and Capacity Model
- Threshold Optimization Decision Curve
- Champion-Challenger Test Record

Day 8: Explain and Prioritize Alerts

- Model Explanation Evidence Pack
- Reason-Code Design and Validation
- Alert Risk and Urgency Prioritization Matrix
- Investigator Capacity Allocation Board
- Customer Friction and Control Tradeoff Log

Day 9: Govern Investigation Handoffs

- Alert-to-Case Handoff Checklist
- Analytical Evidence and Limitation Record
- Case Feedback and Label Correction Loop
- Model Drift and Fraud Change Indicators
- Monitoring, Escalation, and Review Calendar



Day 10: Practice Fraud Analytics Decisions

- Exercise: Convert a Fraud Risk into Analytical Tests
- Exercise: Build Features and Select Detection Methods
- Exercise: Evaluate an Imbalanced Fraud Model
- Exercise: Prioritize Alerts and Prepare a Case Handoff
- Capstone: Fraud Analytics Mining Playbook

Practical Exercises

The course uses suggested activities based on payment, claims, procurement, and digital-commerce scenarios.

- Suggested activity: convert a fraud-risk hypothesis into red flags, data requirements, features, labels, and analytical tests.
- Suggested activity: compare classification, anomaly, and graph methods against evidence quality and investigation needs.
- Suggested activity: select thresholds using detection value, false positives, capacity, and customer-friction evidence.
- Suggested activity: assemble explanations, alert priorities, case handoffs, feedback controls, and monitoring indicators.

FAQs

Who suits advanced fraud analytics training, and what does it assume?

Fraud, investigation, risk, audit, compliance, and data functions suit the training; it assumes participants can analyze structured data, interpret model evidence, and document operational decisions.

How does fraud analytics data mining differ from general data mining strategy?

Fraud analytics data mining concentrates on rare-event labels, evolving behavior, suspicious networks, investigation capacity, evidence handoffs, and monitoring, while general data mining strategy addresses broader pattern-discovery decisions.

How should imbalanced fraud detection models be evaluated?

Imbalanced fraud detection models should be evaluated through ranking quality, precision, recall, calibration, false-positive cost, investigation capacity, segment stability, threshold effects, and performance on untouched validation and holdout samples.

How does fraud network analysis improve suspicious pattern detection?

Fraud network analysis reveals shared identifiers, connected groups, cycles, hubs, indirect links, and coordinated behavior that transaction-by-transaction scoring can miss.



How should fraud alert triage support investigations?

Fraud alert triage should combine risk, urgency, explanation quality, potential impact, available evidence, duplication checks, and investigator capacity into a documented prioritization and handoff process.

Conclusion

Participants take back a Fraud Analytics Mining Playbook containing hypotheses, data controls, features, method choices, validation evidence, thresholds, explanations, triage rules, investigation handoffs, and monitoring indicators. It changes disconnected analytical tests into a governed detection-to-investigation process. The playbook connects fraud-risk decisions with measurable evidence, operational ownership, and feedback.