CONCEPT

AI Fraud Detection and Fraud Analytics: Machine Learning, Anomaly Detection and Alert Triage

AI Fraud Detection and Fraud Analytics: Machine Learning, Anomaly Detection and Alert Triage

Introduction:

AI fraud detection is moving from vendor promise to daily operations, yet many organisations still rely on static rules that flood investigators with false positives while new schemes in payments, procurement, claims and payroll slip through. Machine learning, anomaly detection and link analysis can change that, but only when data, thresholds and investigator workflow are designed together. This Core Concept course prepares managers to specify detection logic, judge model scores and run alert triage without writing code. Participants leave with a Fraud Analytics Pilot Blueprint and business case for their own organisation.

Course Objectives:

- Map fraud typologies in payments, procurement, claims and payroll to the transaction data and behavioural signals that reveal them
- Compare rules-based, supervised machine learning, anomaly detection and network analysis approaches and select the right mix for each fraud scenario
- Specify data sources, feature ideas and labelling needs for a fraud detection model and assess data readiness
- Set risk score thresholds and alert triage rules that balance detection rate, false positives and investigator capacity
- Oversee deployed fraud models for drift, bias and explainability using NIST AI RMF 1.0 and ISO/IEC 42001 as reference
- Produce a Fraud Analytics Pilot Blueprint with KPIs and a business case ready for sponsor approval

Target Audience:

- Managers accountable for fraud prevention and detection programmes in their organisation
- Finance operations and accounts payable managers who own payment and vendor master processes
- Procurement and supply managers responsible for tendering, purchase orders and supplier onboarding
- Claims and benefits managers in insurance, healthcare and public service settings who handle high claim volumes
- Payroll and HR operations managers responsible for employee master data and pay runs
- Analytics and data managers who supply, build or buy detection models for operational teams

Course Outline:

Day 1: Fraud Typologies and the Detection Landscape

- Payment Fraud Patterns: Duplicate Payments, Invoice Redirection and Vendor Bank Detail Changes
- Procurement Fraud Patterns: Bid Rigging, Split Purchases and Shell Supplier Indicators
- Claims Fraud Patterns: Staged, Inflated and Repeat Claims Across Insurance and Benefits
- Payroll Fraud Patterns: Ghost Employees, Overtime Abuse and Unauthorised Pay Changes
- ACFE/SAS Anti-Fraud Technology Benchmarking Report: Adoption of Analytics and AI

Day 2: Detection Approaches and Analytics Architecture

- Rules-Based Detection Versus Machine Learning: Strengths, Limits and Hybrid Designs
- Supervised Classification Models for Fraud Risk Scoring: Gradient Boosting and Random Forest Concepts
- Unsupervised Anomaly Detection: Isolation Forest, Clustering and Peer Group Outliers
- Network and Link Analysis: Entity Resolution and Graph Views of Shared Addresses, Accounts and Devices
- Fraud Analytics Platform Architecture: Batch Scoring, Real-Time Scoring and Case Management Integration

Day 3: Data, Features and Alert Triage in Practice

- Fraud Data Source Inventory: ERP, Payment Files, Claims Systems, HR Master Data and External Watchlists
- Feature Design Ideas: Velocity, Deviation From Peer Baseline, Timing and Relationship Signals
- Label Quality: Confirmed Fraud Outcomes, Class Imbalance and Feedback From Investigators
- Risk Score Thresholds: Precision, Recall and the Confusion Matrix in Operational Terms
- Alert Triage Workflow: Prioritisation Queues, Disposition Codes and Investigator Capacity Planning

Day 4: Model Oversight, Bias and Explainability

- False Positive Reduction: Rule Tuning, Score Segmentation and Suppression Logic
- Model Drift and Fraudster Adaptation: Performance Monitoring Dashboards and Retraining Triggers
- Explainable Alerts: Reason Codes and Feature Contribution Views for Investigators
- Bias and Fairness Checks in Fraud Scoring for Customers, Claimants and Employees
- AI Risk Controls for Fraud Models Using NIST AI RMF 1.0 and ISO/IEC 42001

Day 5: Pilot Case Work and the Fraud Analytics Pilot Blueprint

- Accounts Payable Case: Reviewing Anomaly Alerts on Vendor Payments
- Insurance Claims Network Case: Judging Link Analysis Evidence Before Referral
- Fraud Analytics Pilot Scope, KPIs and Go or No-Go Criteria for an Own Organisation
- Business Case Build: Loss Avoided, Investigator Hours Saved and Platform Costs
- Fraud Analytics Pilot Blueprint Presentation and Peer Challenge

Skills You Will Gain:

- Fraud Typology Mapping
- Detection Method Selection
- Fraud Feature Specification
- Alert Threshold Calibration
- Alert Triage Management
- Fraud Model Monitoring
- Explainable AI Oversight
- Fraud Analytics Business Case Design

Why Attend This Course:

- Return with a Fraud Analytics Pilot Blueprint and business case for a real detection gap in your organisation
- Question vendors and data scientists on detection rates, false positives and model drift in terms investigators understand
- Cut wasted investigator time by redesigning alert queues and disposition feedback before buying new tools
- Compare detection practice with managers from finance, insurance, healthcare, public services, retail and energy sectors

Conclusion:

Fraud detection improves when typologies, data, models and investigator workflow are designed as one system rather than bought as separate tools. This course moves from fraud patterns in payments, procurement, claims and payroll, through rules, machine learning, anomaly detection and link analysis, to features, thresholds and alert triage, and then to drift, bias and explainability. The final day applies these methods to multi-sector cases and produces a Fraud Analytics Pilot Blueprint ready for sponsor review.