



AUDITING AND GOVERNANCE RISK AND COMPLIANCE

AI-Driven Fraud Detection in Banking

Course code: AGRC-019

SPARK TRAINING

Professional training courses for leaders, specialists, and organizations seeking practical capability development.

info@sparktraining.eu

+31 85 115 0004 | sparktraining.eu

— Workshop Overview

Financial fraud represents a significant and evolving threat to the banking industry. The rapid expansion of digital banking, instant payments, mobile financial services, and interconnected financial platforms has created new opportunities for fraudsters to exploit vulnerabilities in banking systems, customer interactions, and transaction processes. Traditional fraud detection systems often rely on predefined rules, manual investigations, and historical fraud patterns. Although these approaches remain important, they can struggle to identify emerging fraud techniques, sophisticated transaction networks, and rapidly changing criminal behaviours. High volumes of false alerts can also overwhelm investigation teams, increase operational costs, and delay legitimate customer transactions. Artificial intelligence (AI), machine learning, and advanced analytics are transforming banking fraud detection by enabling financial institutions to identify unusual transaction patterns, analyse customer behaviour, detect suspicious relationships, and prioritise potentially fraudulent activities more effectively. However, successful AI-driven fraud detection requires more than implementing sophisticated algorithms. Banks must establish reliable data pipelines, select appropriate analytical techniques, evaluate model performance, manage false positives, protect customer information, and ensure that automated detection systems operate within effective governance and regulatory frameworks. The AI-Driven Fraud Detection in Banking course provides banking professionals with a practical understanding of how AI and machine learning can strengthen fraud prevention, detection, investigation, and risk management. Participants explore transaction monitoring, anomaly detection, supervised and unsupervised learning, behavioural analytics, network analysis, model validation, explainable AI, real-time fraud detection, and responsible AI governance. Through realistic banking fraud scenarios, analytical exercises, and implementation workshops, participants develop the capabilities needed to evaluate AI-driven fraud detection solutions and integrate them into banking operations.

Why Attend

The programme combines instructor-led discussions, banking fraud case studies, AI and machine learning demonstrations, analytical workshops, fraud detection simulations, and model governance exercises. Participants work with illustrative banking datasets containing transaction histories, customer behaviour

Who Should Attend

Banking fraud prevention and detection managers
Financial crime compliance professionals
Banking risk management specialists
Anti-money laundering and transaction monitoring analysts
Internal auditors and banking compliance officers
Banking data analysts and data scientists

— Learning Objectives

- Explain the major types of banking fraud and their evolving risk characteristics
- Understand the applications of artificial intelligence and machine learning in fraud detection
- Identify and prepare relevant banking transaction and behavioural data
- Apply supervised and unsupervised learning concepts to fraud detection scenarios
- Understand anomaly detection and behavioural analytics techniques
- Evaluate fraud detection models using appropriate performance metrics
- Develop risk-based fraud scoring and alert prioritisation approaches
- Explain the role of graph analytics in identifying coordinated fraud networks
- Assess real-time fraud detection architectures and operational workflows
- Understand model explainability, validation, and responsible AI requirements
- Integrate AI-generated fraud alerts with investigation and case management processes
- Develop an AI-driven fraud detection implementation and governance roadmap

Course Outline

**DAY
1**

Banking Fraud Landscape and Foundations of AI-Driven Detection

- Understanding the banking fraud landscape, including payment fraud, account takeover, identity fraud, card fraud, authorised push payment scams, and fraudulent account activity
- Examining the limitations of traditional rule-based fraud detection systems and the opportunities presented by AI, machine learning, and advanced analytics
- Exploring the fraud detection lifecycle, including prevention, monitoring, alert generation, investigation, case resolution, and feedback mechanisms
- Understanding the fundamentals of supervised learning, unsupervised learning, anomaly detection, and predictive analytics in banking fraud management
- Identifying relevant fraud data sources, including transaction records, customer profiles, device information, digital channel activity, and historical investigation outcomes
- Practical workshop: Analysing banking fraud scenarios and identifying opportunities for AI-driven detection across customer journeys and payment processes

**DAY
2**

Fraud Data Analytics, Machine Learning and Anomaly Detection

- Preparing banking fraud datasets through data cleaning, validation, integration, transformation, and the handling of missing or inconsistent information
- Developing fraud detection features using transaction frequency, payment amounts, account activity, behavioural deviations, geographic signals, and customer history
- Understanding supervised classification algorithms, including logistic regression, decision trees, random forests, and gradient boosting techniques
- Exploring unsupervised learning methods, including clustering, isolation forests, and anomaly scoring for detecting previously unidentified suspicious patterns
- Addressing class imbalance, limited fraud labels, data leakage, and the challenges of training models on rare fraudulent events
- Analytical workshop: Designing and evaluating a machine learning fraud detection model using illustrative banking transaction data and risk indicators

**DAY
3**

Advanced Fraud Analytics, Behavioural Intelligence and Network Detection

- Applying behavioural analytics to identify deviations from normal customer transaction patterns, account usage, login activity, and payment behaviour
- Understanding graph analytics and network-based detection techniques for identifying suspicious relationships between accounts, devices, beneficiaries, and transactions
- Exploring the use of sequential and temporal analysis to detect unusual transaction sequences, rapid account activity, and coordinated fraud attempts
- Examining AI applications in identity verification, digital onboarding, document fraud detection, and account takeover prevention

- Evaluating fraud risk scoring techniques that combine machine learning outputs, business rules, behavioural signals, and contextual risk information
- Case study: Investigating a simulated coordinated banking fraud network using behavioural indicators, transaction relationships, and risk-based alert prioritisation

DAY
4

Real-Time Fraud Detection, Model Performance and Investigation Integration

- Understanding real-time fraud detection architectures involving transaction data streams, feature generation, model scoring, decision engines, and automated alerts
- Evaluating fraud model performance using precision, recall, F1-score, precision-recall curves, false-positive rates, and financial loss-based measures

- Establishing risk thresholds and decision strategies that balance fraud prevention, customer experience, investigation capacity, and operational costs
- Integrating AI-generated alerts with fraud investigation workflows, case management systems, analyst feedback, and escalation procedures
- Monitoring model performance for data drift, changing fraud patterns, declining detection effectiveness, and the need for model recalibration or retraining
- Practical exercise: Designing a real-time fraud monitoring workflow with model performance indicators, alert thresholds, investigation priorities, and customer protection controls

DAY
5

Responsible AI, Fraud Model Governance and Banking Implementation Strategy

- Establishing governance arrangements for AI-driven fraud detection covering model ownership, validation, documentation, approval, accountability, and independent oversight
- Understanding explainable AI techniques and the importance of interpreting fraud risk scores, model decisions, and contributing risk factors
- Assessing privacy, data protection, fairness, cybersecurity, and third-party technology risks associated with banking AI systems
- Evaluating relevant regulatory and supervisory expectations for financial crime controls, model risk management, operational resilience, and automated decision-making
- Developing implementation roadmaps covering business requirements, data readiness, technology selection, pilot testing, integration, model monitoring, and continuous improvement
- Capstone exercise: Developing and presenting a Comprehensive AI-Driven Banking Fraud Detection Framework incorporating fraud risk assessment, data architecture, machine learning techniques, behavioural analytics, fraud scoring, real-time monitoring, investigation workflows, model governance, and implementation priorities

— Upcoming Classroom Dates

Schedule available on request. Contact SPARK Training for current dates, locations, and fees.

— Certificate and Registration

Participants who attend and complete the full programme receive a SPARK Training Certificate of Completion. For registration, in-house delivery, or availability questions, contact info@sparktraining.eu or +31 85 115 0004.