Fraud Analytics with SQL and Python Training Course

Professional Development Training Course Outline

Category	Risk Management	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The exponential rise in Financial Crime and sophisticated Cyberattacks has made modern Fraud Detection and Risk Management a critical, data-intensive challenge for all industries. Traditional, rule-based systems are failing to keep pace with dynamic fraud schemes, creating an urgent demand for skilled professionals who can leverage Big Data Analytics and Machine Learning (ML). Fraud Analytics with SQL and Python Training Course is specifically designed to bridge that skills gap by providing a rigorous, hands-on mastery of the two foundational technologies in the modern data ecosystem: SQL for robust data extraction and manipulation, and Python for advanced statistical modeling and automation.

This intensive program goes beyond theory, focusing on Applied Data Science to deliver tangible, high-impact Fraud Prevention solutions. Participants will learn to architect and implement end-to-end analytical pipelines, from structuring complex datasets in Relational Databases using efficient SQL queries to deploying cutting-edge Predictive Models using Python libraries like Pandas, Scikit-learn, and TensorFlow. By mastering Anomaly Detection, Transactional Monitoring, and Behavioral Biometrics across real-world case studies, attendees will be equipped to transform reactive investigation into proactive Continuous Monitoring, significantly strengthening their organization's Anti-Fraud Framework and driving tangible Loss Mitigation in the age of digital transactions.

Programme Curriculum

Fraud Analytics with SQL and Python Training Course

Introduction

The exponential rise in Financial Crime and sophisticated Cyberattacks has made modern Fraud Detection and Risk Management a critical, data-intensive challenge for all industries. Traditional, rule-based systems are failing to keep pace with dynamic fraud schemes, creating an urgent demand for skilled professionals who can

leverage Big Data Analytics and Machine Learning (ML). Fraud Analytics with SQL and Python Training Course is specifically designed to bridge that skills gap by providing a rigorous, hands-on mastery of the two foundational technologies in the modern data ecosystem: SQL for robust data extraction and manipulation, and Python for advanced statistical modeling and automation.

This intensive program goes beyond theory, focusing on Applied Data Science to deliver tangible, high-impact Fraud Prevention solutions. Participants will learn to architect and implement end-to-end analytical pipelines, from structuring complex datasets in Relational Databases using efficient SQL queries to deploying cutting-edge Predictive Models using Python libraries like Pandas, Scikit-learn, and TensorFlow. By mastering Anomaly Detection, Transactional Monitoring, and Behavioral Biometrics across real-world case studies, attendees will be equipped to transform reactive investigation into proactive Continuous Monitoring, significantly strengthening their organization's Anti-Fraud Framework and driving tangible Loss Mitigation in the age of digital transactions.

Course Duration

5 days

Course Objectives with Trending Keywords

1. Efficiently write and optimize complex SQL Queries to extract, transform, and load large-scale Transactional Data for fraud analysis.
2. Utilize core Python libraries for robust Data Wrangling, cleaning, and Exploratory Data Analysis (EDA) on raw financial datasets.
3. Apply unsupervised Machine Learning techniques to identify statistically significant Outliers and emerging Fraud Patterns.
4. Build and tune supervised Classification Models for high-accuracy Credit Card Fraud Detection and risk scoring.
5. Critically assess model efficacy using appropriate Metrics for highly Imbalanced Datasets.
6. Perform Network Analysis and graph-based techniques to map complex relationships and uncover Collusive Fraud or Mule Networks.
7. Strategically create high-impact Risk Indicators and Predictive Features from raw data to maximize model performance in a Real-Time context.
8. Incorporate User Behavior and Biometrics to establish baseline profiles and detect deviations indicative of Account Takeover (ATO) fraud.
9. Use Python's Matplotlib and Seaborn to create compelling Fraud Dashboards for effective Data Storytelling to executive stakeholders.
10. Understand the role of analytics in meeting AML (Anti-Money Laundering) and KYC (Know Your Customer) compliance and reporting requirements.
11. Architect a robust system for Automated and Scalable fraud screening and alert generation leveraging scheduled Python scripts and SQL views.
12. Detail techniques for addressing specific fraud types like Chargeback Fraud and Synthetic Identity Fraud in digital commerce environments.
13. Translate complex analytical findings into actionable Investigative Leads and implement evidence-based Control Recommendations.

Target Audience

1. Fraud Analysts and Fraud Investigators
2. Risk Management and Compliance Officers.

3. Data Analysts and Business Intelligence (BI) Professionals.
4. Internal Auditors.
5. Forensic Accountants.
6. Credit Risk Professionals and Underwriters.
7. FinTech and E-commerce Security Specialists.
8. Data Scientists.

Course Modules

Module 1: Data Foundations and SQL for Fraud Data

- Introduction to the Fraud Data Lifecycle and common data sources
- Advanced SQL for data preparation.
- Creating a Star Schema for efficient fraud reporting and analysis in a relational database.
- Data Quality and Normalization techniques using SQL to prepare dirty datasets for modeling.
- Case Study: Vendor Fraud: Using SQL joins and grouping to find patterns in duplicate vendor names, addresses, and payment amounts in a procurement dataset.

Module 2: Python Environment and Exploratory Data Analysis (EDA)

- Setting up the Python environment
- Data Import/Export and initial data cleaning
- Exploratory Data Analysis
- Calculating summary statistics and identifying transaction concentration and velocity.
- Case Study: E-commerce Card Testing: Utilizing Pandas to analyze a high-volume transaction log for rapid, small-value transactions from a limited set of IPs/Devices.

Module 3: Feature Engineering and Data Preprocessing

- Feature Scaling and Encoding for ML algorithms.
- Creating Aggregate Features
- Techniques for handling Categorical Features with high cardinality
- Managing the extreme imbalance of fraud data through Sampling Techniques
- Case Study: Insurance Claim Fraud: Engineering features like 'claim-to-policy age ratio' and 'average claim amount by adjuster' to identify suspicious claims.

Module 4: Supervised Machine Learning for Predictive Fraud

- Introduction to Classification Algorithms
- Training, testing, and cross-validation for building a robust Predictive Model.
- Hyperparameter tuning and feature selection for optimizing model performance.
- Model interpretation using tools like SHAP and Feature Importance for explainability.
- Case Study: Credit Application Fraud.

Module 5: Unsupervised Anomaly Detection

- Principles of Unsupervised Learning and its role in catching Zero-Day Fraud schemes.
- Implementing Clustering Algorithms to group transactions and flag small, suspicious clusters.
- Practical application of Isolation Forest and Local Outlier Factor for spotting anomalies in high-dimensional data.
- Understanding the trade-off between False Positives and False Negatives in anomaly models.
- Case Study: Internal Theft.

Module 6: Time-Series Analysis and Deep Learning Fundamentals

- Analyzing Time-Series patterns in fraud data
- Introduction to basic Deep Learning models for complex pattern recognition.
- Implementing a simple Autoencoder for Outlier Detection in transactional sequences.
- Sequential analysis of customer journeys and session logs for Session Hijacking attempts.
- Case Study: Loyalty Program Fraud.

Module 7: Network Analysis and Visualization

- Introduction to Graph Theory and its application in mapping Fraud Networks
- Using Python libraries to create and visualize graph data structures from transactional records.
- Calculating key Network Metrics to identify central "Mules" and collaborators.
- Integrating network features as powerful predictors into the supervised ML model.
- Case Study: Money Mule Detection.

Module 8: Operationalization and Reporting

- Introduction to Model Deployment concepts and generating real-time Risk Scores.
- Developing and automating a Continuous Monitoring data pipeline using Python scripts and SQL triggers.
- Creating compelling Data Visualizations and interactive Fraud Dashboards
- Establishing an Alert Triage and Case Management workflow based on model output.
- Case Study: Alert Prioritization.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com