Payment Fraud Prevention for Banks Training Course

Professional Development Training Course Outline

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

Course Introduction

In an era where agentic AI and generative AI are industrializing financial crime, banks face an unprecedented surge in synthetic identity fraud and cross-channel manipulation. Payment Fraud Prevention for Banks Training Course empowers financial institutions to pivot from static, rule-based defenses to real-time behavioral analytics and dynamic risk orchestration. By fostering a culture of "ownership of fraud," the curriculum ensures that your frontline and back-office teams can neutralize sophisticated threats before they compromise institutional integrity.

Through immersive, role-specific simulations, participants will master the ability to detect subtle behavioral deviations and execute fraud-resilient protocols. This is not merely a compliance exercise; it is a strategic imperative to safeguard capital, enhance customer trust, and maintain operational resilience against the next generation of automated, high-velocity financial attacks.

Programme Curriculum

Payment Fraud Prevention for Banks Training Course

Introduction

In an era where agentic AI and generative AI are industrializing financial crime, banks face an unprecedented surge in synthetic identity fraud and cross-channel manipulation. Payment Fraud Prevention for Banks Training Course empowers financial institutions to pivot from static, rule-based defenses to real-time behavioral analytics and dynamic risk orchestration. By fostering a culture of "ownership of fraud," the curriculum ensures that your frontline and back-office teams can neutralize sophisticated threats before they compromise institutional integrity.

Through immersive, role-specific simulations, participants will master the ability to detect subtle behavioral deviations and execute fraud-resilient protocols. This is not merely a compliance exercise; it is a strategic imperative to safeguard capital, enhance customer trust, and maintain operational resilience against the next generation of automated, high-velocity financial attacks.

Course Duration

5 days

Course Objectives

1. Master real-time behavioral biometrics to detect fraudulent patterns.
2. Identify and mitigate risks associated with agentic AI and automated deepfakes.
3. Deploy layered ID validation to counter sophisticated synthetic identity fraud.
4. Implement cross-channel data integration to break down operational silos.
5. Execute effective "Stop, Call, Confirm" protocols for real-time payment security.
6. Understand the convergence of AML (Anti-Money Laundering) and fraud prevention strategies.
7. Analyze contextual signals during high-friction transaction monitoring.
8. Recognize social engineering and authorized push payment (APP) scam tactics.
9. Strengthen internal control systems through rigorous segregation of duties.
10. Navigate evolving regulatory compliance landscapes
11. Build an institutional culture centered on proactive fraud awareness.
12. Leverage machine learning orchestration to reduce false positive rates.
13. Apply forensic investigation techniques to analyze near-misses and breaches.

Target Audience

- Frontline Branch Tellers & Customer Service Representatives
- Loan Officers & Credit Underwriting Specialists
- Financial Crimes & AML Compliance Officers
- Cybersecurity & Digital Security Analysts
- Branch Managers & Operational Supervisors
- Internal Audit & Risk Management Teams
- Payment Operations & Treasury Specialists
- Senior Management & Board Oversight Committees

Training Modules

1. The 2026 Threat Landscape

- Evolution of AI-driven financial crimes.
- Understanding the "All Green" authentication trap.
- The mechanics of agentic AI automation.
- Impact of high-velocity real-time payments.
- *Case Study:* Analyzing a multi-channel attack that bypassed traditional firewalls.

2. Synthetic Identity & Onboarding Security

- Deep-dive into AI-generated fake identity documents.
- Dynamic verification beyond the point of onboarding.
- Combining device intelligence with document forensics.
- Identifying "sleeper" accounts and long-game fraud.

- *Case Study:* Tracking a synthetic identity ring that operated for 18 months.

3. Behavioral Biometrics & Pattern Recognition

- Detecting hesitation and anomalies in user navigation.
- Mapping cross-channel behavioral signals.
- Differentiating legitimate user friction from manipulation.
- Implementing adaptive risk scoring.
- *Case Study:* Using behavioral signals to stop a compromised account takeover.

4. Real-Time Payment Protection

- Strategies for irreversible transaction environments.
- Identifying "mule" account behavior in real-time.
- Orchestrating trust signals across digital wallets.
- Balancing user friction with transaction velocity.
- *Case Study:* Intercepting a high-value instant credit transfer in milliseconds.

5. Social Engineering & APP Scams

- Psychology of manipulation and urgency.
- Advanced phishing and business email compromise (BEC).
- Protecting vulnerable segments of the customer base.
- The role of "Stop, Call, Confirm" workflows.
- *Case Study:* Preventing an executive-impersonation transfer during a live crisis.

6. Converging Fraud & AML

- Integrating siloed data streams for holistic visibility.
- Linking fraud detection with money laundering trails.
- Strategic importance of unified data architecture.
- Regulatory reporting requirements in a high-speed era.
- *Case Study:* How shared intelligence stopped a coordinated money-laundering network.

7. Internal Controls & Fraud Culture

- Enforcing strict segregation of duties in payments.
- Empowering staff to escalate without fear of reprisal.
- Continuous monitoring of insider threat indicators.
- Creating a "Fraud-Resilient" organizational mindset.
- *Case Study:* Uncovering internal fraud by identifying abnormal approval patterns.

8. Incident Response & Forensic Analysis

- Rapid response procedures for confirmed breaches.
- Post-mortem analysis and learning loops.
- Communicating with stakeholders and regulators.
- Leveraging forensic tools to prevent repeat attacks.
- *Case Study:* A comprehensive post-breach audit that updated 2026 security protocols.

Training Methodology

- 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
07 Sep 2026	11 Sep 2026	Online	$1,000
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Online	$1,000
14 Sep 2026	18 Sep 2026	Physical	$1,500

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Online	$1,000
28 Sep 2026	02 Oct 2026	Physical	$1,500

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

Register Online Now

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