MANAGING FRAUD IN A DIGITIZED WORLD



GENTEX®
TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Introduction

The Managing Fraud in a Digitized World Training Course prepares professionals to control fraud risk as transactions, identities, and communications move online. Digitalisation expands reach and speed, and it also expands the fraudster's toolkit. Synthetic identities, account takeover, authorised push payment scams, deepfake impersonation, and business email compromise now sit alongside traditional schemes. This course explains how those attacks work and how organisations detect, prevent, and investigate them. It covers digital identity, payment fraud, analytics, and cyber-fraud convergence. Furthermore, it applies regulatory duties and evidence standards. As a result, participants manage digital fraud exposure with confidence.

Managing Fraud in a Digitized World Course Objectives

- Explain how digitalisation changes fraud risk and control needs.
- Identify digital fraud typologies including synthetic identity and account takeover.
- Assess authorised push payment, phishing, and social engineering risks.
- Apply identity verification, onboarding, and authentication controls.
- Evaluate payment fraud controls across cards, transfers, and wallets.
- Apply data analytics, device intelligence, and behavioural monitoring.
- Assess deepfake, business email compromise, and impersonation fraud risks.
- Apply cyber-fraud convergence and third-party risk controls.
- Investigate digital fraud with evidence handling and documentation.
- Apply regulatory duties including reporting, liability, and consumer protection.

Course Methodology

- Interactive lectures with real digital fraud and breach case studies.
- Fraud typology and control mapping workshops.

GENTEX® TRAINING CENTER

- Device intelligence, behavioural analytics, and monitoring exercises.
- Digital fraud investigation simulation covering evidence and reporting.
- Structured peer discussion with facilitator feedback on fraud programme design.

Who Should Take This Course

- Fraud, risk, and financial crime professionals.
- Digital banking and payment operations teams.
- Information security and cyber-fraud analysts.
- Compliance and consumer protection officers.
- Internal auditors covering digital fraud controls.
- Product managers for digital channels and payments.

Managing Fraud in a Digitized World Course Outlines

Day 1: The Digital Fraud Landscape

- How digitalisation changes fraud opportunity, scale, and speed.
- Digital fraud typologies and emerging attack patterns.
- Channels at risk: web, mobile, APIs, wallets, and instant payments.
- Organised crime groups and fraud-as-a-service models.
- Regulatory landscape and supervisory expectations.
- Fraud governance, appetite, and programme structure.
- Case study: a digital fraud attack and the control response.

Day 2: Identity, Onboarding, and Authentication

- Synthetic identity, identity theft, and impersonation risks.

- Identity document verification and biometric checks.
- Anti-impersonation and liveness detection basics.
- Strong customer authentication and multi-factor methods.
- Account takeover detection and step-up authentication.
- Know your customer and beneficial ownership verification.
- Workshop: designing onboarding and authentication controls.

Day 3: Payment Fraud and Scam Prevention

- Card-not-present fraud and card testing attacks.
- Authorised push payment scams and liability frameworks.
- Business email compromise and invoice redirection fraud.
- Mule accounts, layering, and money movement patterns.
- Faster payment risk and recovery limitations.
- Consumer warnings, confirmation of payee, and scam intervention.
- Workshop: mapping payment fraud controls across a channel.

Day 4: Analytics, Device Intelligence, and Monitoring

- Digital fraud analytics and detection model design.
- Device fingerprinting, device intelligence, and emulator detection.
- Behavioural biometrics, session analysis, and velocity checks.
- Network and link analysis across accounts and devices.
- Real-time decisioning and rule-model hybrid design.
- Managing false positives and customer friction.
- Workshop: designing a digital fraud monitoring approach.

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Day 5: Investigation, Reporting, and Compliance

- Digital fraud investigation planning and scoping.
- Evidence handling, logs, and chain of custody basics.
- Working with law enforcement and industry bodies.
- Regulatory reporting, liability, and consumer redress.
- Cyber-fraud convergence and third-party risk controls.
- Awareness programmes and customer education.
- Course review, assessment, and action planning.

Conclusion

By successfully completing Managing Fraud in a Digitized World, participants will gain a thorough understanding of digital fraud typologies, identity and authentication controls, payment fraud prevention, analytics and device intelligence, investigation practice, and regulatory duties. They will also acquire practical skills in control mapping, scam prevention design, monitoring analytics, and digital fraud investigation. In addition, the course prepares them to reduce digital fraud exposure across channels. Gentex Training Center delivers this programme with a strong focus on applied digital fraud practice and measurable loss reduction.

FAQs for Managing Fraud in a Digitized World course

GENTEX® TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Q1 What is the "Managing Fraud in a Digitized World" course about?

It is a five-day programme on managing fraud risk in digital channels. It covers digital fraud typologies, identity verification and authentication, payment and scam fraud, analytics and device intelligence, cyber-fraud convergence, investigation practice, and regulatory duties including reporting and liability.

Q2 What are the key benefits of the "Managing Fraud in a Digitized World" course?

Participants learn how digital fraud actually works, which allows controls to be placed where losses occur. The course reduces scam and account takeover losses, strengthens onboarding and authentication, improves detection with less customer friction, improves investigation and evidence quality, and supports compliance with reporting and liability obligations.

Q3 What skills will I gain from the "Managing Fraud in a Digitized World" course?

Participants gain digital fraud typology assessment and control mapping, identity verification and authentication control design, payment fraud and scam prevention design, and digital fraud monitoring analytics with investigation and reporting. These four skills cover the practical core of digital fraud management.

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Q4 What tools, methods, or standards are covered in the "Managing Fraud in a Digitized World" course?

The course covers digital fraud typologies including synthetic identity, account takeover, phishing and authorised push payment scams, digital identity document verification and biometric checks, liveness and anti-impersonation detection, strong customer authentication and multi-factor methods, step-up authentication, device fingerprinting and emulator detection, behavioural biometrics and session analysis, velocity checks, network and link analysis, real-time decisioning and rule-model hybrid design, card-not-present and card testing controls, business email compromise detection, mule account and layering analysis, confirmation of payee and scam intervention tools, false positive management, digital evidence handling and chain of custody, law enforcement and industry body cooperation, regulatory reporting and liability frameworks, consumer redress, and third-party risk controls.

Q5 How is the "Managing Fraud in a Digitized World" course applied in real-world practice?

Participants apply the methods in their own fraud programmes. They map digital fraud exposure by channel, design onboarding and payment controls, configure monitoring rules and models, review scam intervention points, plan investigations, document findings, and prepare regulatory reports. Many leave with a digital fraud control matrix and a monitoring design outline ready for immediate use.