CONCEPT

# Deepfake Fraud Defence: Synthetic Media Detection and AI Identity Fraud Prevention

# Deepfake Fraud Defence: Synthetic Media Detection and AI Identity Fraud Prevention

**Technical depth:** Practitioner · **Practical mode:** Simulation

## Introduction

Generative tools now let criminals clone a voice from a short recording, inject a synthetic face into a remote identity check and fabricate documents that pass a visual review. Fraud, onboarding and payment controls built on recognising a familiar voice or face are losing their value, and many organisations discover the gap only after a transfer has been made. This coreconcept course equips operational teams to detect, verify and respond to synthetic media attacks using recognised biometric and incident standards. Participants work through timed attack scenarios and leave with a Deepfake Fraud Defence Playbook for their own organisation.

## Course Objectives

- Classify synthetic media and deepfake fraud typologies and map where they can enter onboarding, payment and communication channels
- Apply presentation and injection attack detection standards, including ISO/IEC 30107-3 and CEN/TS 18099, when specifying or testing identity verification controls
- Verify suspect audio, video and images using forensic checklists, content provenance data and out-of-band confirmation protocols
- Design payment and access controls that remain effective when a caller's voice or face can no longer be trusted
- Respond to a suspected deepfake attack, preserving evidence and coordinating the incident in line with ISO/IEC 27035-1
- Produce a Deepfake Fraud Defence Playbook ready for adoption by fraud, security and finance teams

## Target Audience

- Fraud prevention and investigation staff handling impersonation and identity fraud cases
- Identity verification and customer onboarding teams operating remote proofing and liveness checks
- Security operations and incident response staff who triage social engineering attacks
- Finance, treasury and payment operations staff who approve transfers and supplier bank detail changes
- Contact centre and customer authentication staff exposed to voice impersonation
- Communications and brand protection staff who respond to synthetic media targeting the organisation

## Course Outline

## Day 1: Synthetic Media and the Fraud Threat Landscape

- Synthetic Media Taxonomy: Face Swap, Lip Sync, Voice Clone and Fully Generated Media
- Generative Techniques Overview: GANs, Diffusion Models and Neural Voice Synthesis
- Deepfake Fraud Typologies: Executive Impersonation, Synthetic Identity and Account Takeover
- Attacker Toolkits: Face-Swap Apps, Virtual Camera Software and Fraud-as-a-Service
- Current-State Exposure Assessment Using a Fraud Touchpoint Map

## Day 2: Detection Standards and Provenance Frameworks

- ISO/IEC 30107-3 Presentation Attack Detection Testing and APCER and BPCER Metrics
- CEN/TS 18099 Biometric Data Injection Attack Detection
- NIST SP 800-63-4 Identity Assurance Levels and Remote Proofing Controls
- C2PA Content Credentials and Provenance Manifests
- MITRE ATLAS Techniques for Adversarial Use of AI

## Day 3: Verification and Detection in Daily Operations

- Forensic Media Analysis Checklist: Visual, Audio and Metadata Artefacts
- Liveness Detection Configuration: Active and Passive Challenge Methods
- Out-of-Band Callback and Code-Word Verification Protocols
- Payment Approval Controls: Dual Authorisation and Change-of-Bank-Details Checks
- Detection Tool Evaluation Scorecard: Accuracy, False Rejection and Explainability

## Day 4: Threat Modelling, Incident Handling and Resilience

- STRIDE Threat Modelling of Onboarding and Contact Centre Channels
- Deepfake Fraud Risk Register Aligned to ISO 31000
- Synthetic Media Incident Handling per ISO/IEC 27035-1
- Evidence Preservation and Chain-of-Custody Procedure for Suspect Media
- Detector Evasion, Model Drift and Red-Team Testing Plans

## Day 5: Attack Simulations and the Defence Playbook

- Voice-Clone Payment Fraud Simulation: Cloned Executive Requesting an Urgent Transfer
- Remote Onboarding Simulation: Injected Deepfake Video in Account Opening
- Post-Incident Review Using Timeline and Control-Failure Analysis
- Deepfake Fraud Defence Playbook Drafting
- Playbook Walkthrough and Peer Challenge

## Skills You Will Gain

- Synthetic Media Forensics
- Biometric Attack Detection
- Identity Proofing Assurance
- Social Engineering Resistance
- Payment Fraud Control
- Deepfake Incident Handling
- Detection Tool Evaluation
- Digital Evidence Handling

## Why Attend This Course

- Leave with a Deepfake Fraud Defence Playbook covering channel exposure, verification protocols and a response runbook
- Rehearse under time pressure the decisions that interrupt a cloned-voice or deepfake video fraud while it is still unfolding
- Ask identity verification and detection vendors precise questions about what their testing does and does not cover
- Exchange attack patterns and control lessons with fraud and security staff from banking, government, telecoms and retail

## Conclusion

Deepfake fraud succeeds where controls still assume that seeing or hearing a person proves who they are. This course moves from the techniques and fraud typologies behind synthetic media, through the standards that govern presentation and injection attack detection, to the verification, payment and incident controls that hold under pressure. The final day tests those controls in timed simulations and consolidates them into a Deepfake Fraud Defence Playbook, giving participants a documented and rehearsed response to take back to their fraud, security and finance colleagues.