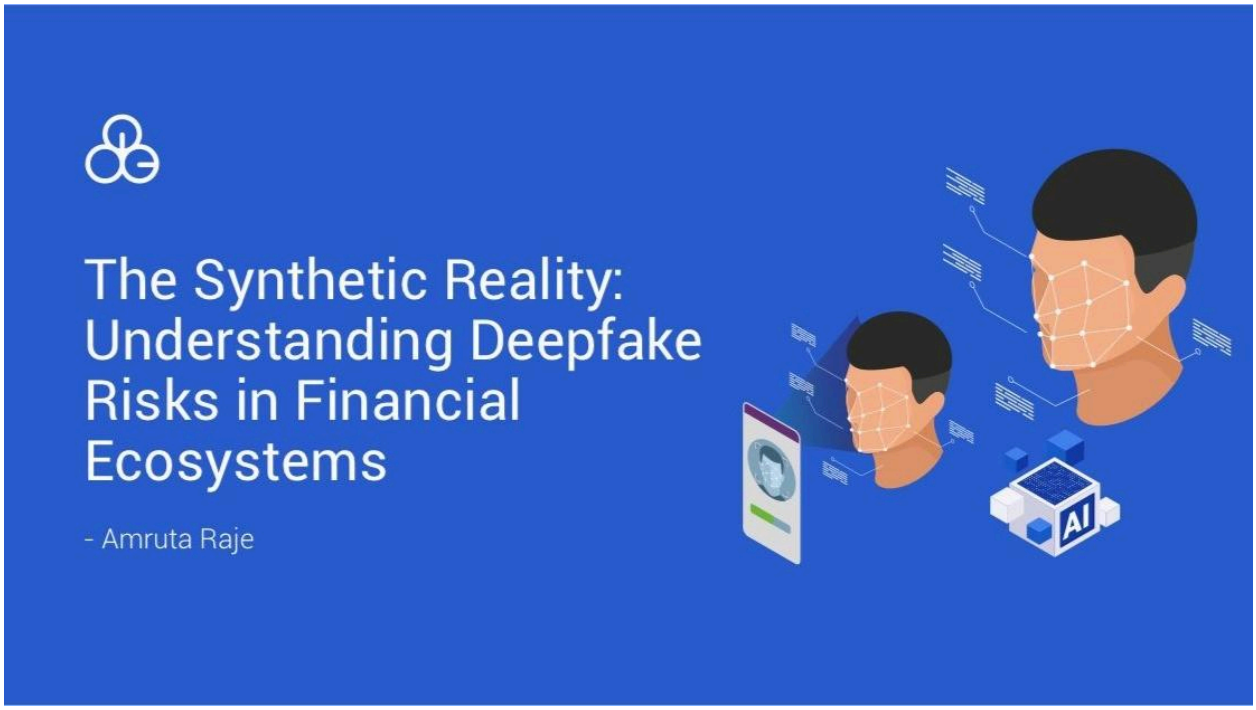

The Synthetic Reality: Understanding Deepfake Risks in Financial Ecosystems

May, 2026

The rapid maturation of Generative AI has moved Deepfakes from the realm of entertainment into a central tool for organised financial crime. Fraudsters have been continuously adapting their techniques alongside technological advancements. As financial systems, digital onboarding platforms, and payment infrastructures evolve, criminals increasingly exploit AI, particularly deepfake technologies, to bypass safeguards designed to prevent money laundering and terrorist financing.

AI-enabled deepfakes are highly convincing synthetic media (video, image, audio) created with deep learning to mimic real people's appearance, voice, or actions. Traditional money laundering relies on manual processes, physical cash, and rule-based monitoring

environments. At the same time, AI-enabled financial crime increasingly leverages synthetic identities, automated mule networks, and sophisticated algorithms to mimic legitimate behaviour and exploit the financial system.

The use of Deepfakes is rapidly increasing, mainly due to their easy, rapid accessibility enabled by generative AI. This enables criminals/fraudsters to conduct financial crime at scale, in a sophisticated manner and poses a challenge in the fight against Money Laundering/Terrorist Financing (TF).

Impact of Deepfakes on AML controls

The following outlines some key emerging trends and associated risks-

● Compromise of Digital KYC and Biometric Verification - AI-enabled deepfakes/synthetic media pose a challenge for KYC compliance, particularly in Customer Due Diligence (CDD) processes, such as ID verification and biometric authentication. The widespread adoption of facial recognition and video-based KYC has created new vulnerabilities, as deepfakes can convincingly replicate facial movements, speech, and other biometric traits, enabling criminals to manipulate authentication processes. Fraudsters can generate synthetic biometric artefacts that can bypass facial recognition, liveness detection, and remote video-KYC verification mechanisms. The misuse of deepfake images and video-conference impersonation techniques is therefore emerging as a significant trend within the evolving financial crime landscape.

● Synthetic Identity creation and Mule account creation - Using synthetic media, fraudsters/Criminals use deepfake faces or voices with stolen or fake personal information. These synthetic identities, further used to open accounts, bypass the identity verification stage and make it complex to trace the origin of illicit funds, as these accounts serve as intermediaries in complex money laundering networks. These

synthetic identities are frequently used as first-layer placement channels within mule account networks, enabling rapid layering across digital payment ecosystems, gaming platforms, and cross-border transfers.

In recent global cases, fraudsters have used deepfake overlays during live video-KYC sessions to impersonate legitimate customers and successfully open mule accounts later used to layer proceeds from cyber-enabled fraud schemes.

To effectively counter the growing threat of AI-enabled deepfakes, financial institutions can implement advanced detection systems that are capable of identifying and responding to these sophisticated, automated behaviours.

AML Controls to Detect Deepfake-Enabled Synthetic Identity and Impersonation Risks:

● Behavioural Monitoring Controls- Monitoring behavioural inconsistencies between onboarding identity attributes and subsequent transaction behaviour can help detect synthetic identities early in the customer lifecycle.

● AI-driven detection tools - Biometric analysis detection can help identify synthetic media and fraudulent identities in real time.

● Strengthening EDD for high-risk profiles- Financial institutions are required to comply with strict CDD and EDD norms, verifying the identity of the customers and beneficial owners, and avoiding manipulation using synthetic media. Enhanced Due Diligence should be prioritised for customers onboarded through non-face-to-face channels where deepfake manipulation risks are inherently higher.

International standard-setting bodies are increasingly recognising deepfake risks within financial crime ecosystems, particularly in relation to digital onboarding fraud, impersonation schemes, and scalable mule account creation. AI-enabled technologies like deepfakes are changing the financial crime landscape, requiring financial institutions to adapt their AML/CFT frameworks toward technology-enabled detection strategies capable of identifying synthetic identities, automated mule networks, and impersonation-driven laundering risks.

Quantum Data Engines™

Quantum Data Engines is a reg-tech company that helps financial institutions detect, manage, and report financial crime more effectively and efficiently.

For more details write to: connect@qde.ai