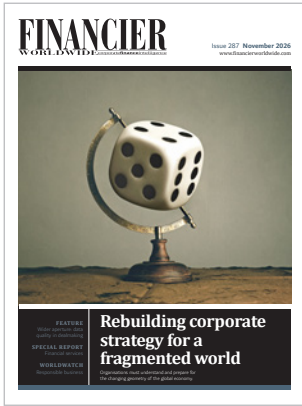




This article first appeared in the November 2026 issue of Financier Worldwide magazine.

© 2026 Financier Worldwide Ltd. All rights reserved. Permission to use this reprint has been granted by the publisher.



■ TALKINGPOINT REPRINT November 2026

AI, deepfakes and financial crime

FW discusses AI, deepfakes and financial crime with Steven Taylor at BDO.



THE RESPONDENT



STEVEN TAYLOR

Forensics – Cyber Risk & Resilience
Director
BDO USA, P.C.
T: +1 (512) 477 7900
E: setaylor@bdo.com

Steve Taylor leads BDO's cyber risk & resilience offering, where he focuses on designing and implementing cyber security strategies for organisations across the public and private sectors. With over 20 years of experience, he serves as a trusted adviser to CISOs and executive leaders, helping them strengthen cyber resilience, navigate regulatory compliance and respond effectively to cyber attacks. His advisory work focuses on translating complex cyber risks into actionable business strategies.

FW: How have AI-generated fraud schemes, synthetic identities and deepfake technologies changed the financial crime landscape over the past two to three years? What developments concern you most today?

Taylor: Artificial intelligence (AI) has lowered the barrier to financial crime. Attacks that once required advanced technical skills and a production team can now be carried out with low-cost or open-source tools. Fraudsters can clone voices, create synthetic identities and automate fraud at scale. This puts advanced capabilities in the hands of inexperienced actors while making seasoned fraudsters even more effective. Over the past several years, financial crime has evolved from manual schemes to highly scalable, AI-enabled operations capable of targeting thousands or even millions of individuals and organisations simultaneously.

Generative AI has accelerated the creation of convincing communications, fraudulent documentation and realistic digital personas while enabling fraudsters to stay one step ahead.

FW: Which AI-enabled fraud techniques are currently proving most effective against organisations? Why are traditional controls struggling to keep pace?

Taylor: Voice cloning and deepfake videos are among the most effective fraud techniques today because they exploit trust and urgency rather than weaknesses in security systems. Many organisations still approve financial transactions through phone calls or video meetings and if a fraudster can convincingly impersonate an executive, those controls may fail. AI-generated phishing and business email compromise attacks are also a growing concern because they

can copy writing styles, business context and communication patterns. These attacks can change quickly and be launched at scale, making it hard for traditional security tools and controls to keep up.

FW: How significant is the threat posed by synthetic identities? What makes this form of fraud particularly difficult to detect and investigate?

Taylor: Synthetic identity fraud is a significant threat because it blends real information with fake names and AI-generated images. It is increasingly hard to detect because there may be no real victim to report the fraud. Fraudsters can build a normal credit history over time, draw down available credit and disappear before the financial institution (FI) recognises the pattern. What makes this form of fraud particularly challenging is that it often appears legitimate

throughout much of the customer lifecycle. Fraudsters can patiently establish credibility over months or even years through positive payment histories and normal account activity. By the time suspicious behaviour emerges, losses may already span multiple products or FIs. The absence of a clear victim, combined with increasingly sophisticated AI-generated documents and images, further complicates detection, investigation and attribution efforts.

FW: To what extent are deepfakes changing the nature of social engineering, executive impersonation and payment fraud risks?

Taylor: Deepfakes make executive impersonation far more convincing. Instead of relying on a suspicious email, a bad actor can use a short public video to recreate an executive's voice and appearance. A live call that appears to come from an executive can make an urgent payment request seem legitimate. This removes many of the warning signs employees have been trained to spot and turns trusted communication channels into a source of risk. Deepfakes represent a significant evolution in social engineering because they enable attackers to simulate credibility rather than simply claim it. As organisations increasingly operate in remote and hybrid environments, employees may have fewer opportunities to validate requests in person. The

result is a growing need to move beyond assumptions that seeing or hearing someone is sufficient proof of identity and instead implement stronger verification procedures.

FW: What practical weaknesses in onboarding, know your customer and identity verification processes are fraudsters increasingly exploiting through AI and deepfake tools?

Taylor: A major weakness is treating identity verification as a one-time onboarding step. Basic video checks, such as asking someone to blink or turn their head, can be bypassed with software that maps a synthetic face onto real movements or a live person. Organisations also rely too heavily on images of physical documents

as a means of verifying someone's identity. AI can generate realistic identification that passes standard verification checks. Fraudsters are also exploiting gaps between onboarding, ongoing authentication and account monitoring processes. Many organisations perform extensive identity checks at account opening but limited verification afterward. As AI-generated documents and synthetic media become increasingly sophisticated, organisations must move beyond static verification methods and adopt continuous monitoring, behavioural analytics and risk-based authentication methods.

FW: What are the most effective prevention and detection measures organisations should be implementing now to



Voice cloning and deepfake videos are among the most effective fraud techniques today because they exploit trust and urgency rather than weaknesses in security systems.

STEVEN TAYLOR
BDO USA, P.C.

strengthen resilience against AI-driven financial crime?

Taylor: Organisations need layered controls that operate throughout the customer lifecycle, not just at onboarding. Active liveness checks should require unpredictable actions that prerecorded videos cannot anticipate. Security teams should also examine file metadata rather than rely on visual review alone. Behavioural analytics can provide another layer by flagging hidden network connections, automated scripts and other suspicious activity. Beyond individual technologies, organisations should adopt a defence in depth strategy that combines people, processes and technology. High-risk transactions should include multiple forms of verification as well as independent approval workflows. Employee

education remains critical because many AI-enabled attacks continue to target human judgment rather than security weaknesses.

FW: If organisations are planning for the future of financial crime risk today, which AI-driven threats should be highest on their agenda?

Taylor: Autonomous fraud networks should be high on the agenda. Today, AI mostly supports human-led attacks and, in the near future, autonomous agents may test controls, learn from failed attempts and change tactics in real time. Human teams cannot operate at that speed or scale, requiring organisations to implement automated defences powered by AI. However, AI amplifies professional judgment. Automated defences handle the

sheer volume of attacks so human investigators are free to apply critical judgment to complex cases. Organisations should also prepare for the convergence of autonomous systems, synthetic identities and deepfake technologies. Together, these capabilities could automate large portions of the fraud lifecycle, from identity creation and account opening to transaction execution and evasion of detection controls. ■

Enjoyed this article?

Join our community for free to access more expert insights.

Join Now - It's Free