# Gambling industry urged to tighten defences against AI-enabled fraud and deepfakes



The growing sophistication of artificial intelligence (AI) technologies is presenting new challenges for gambling operators, particularly with the rise of AI-enabled fraud and identification deepfakes. These developments are increasing risks related to money laundering and fraud, prompting calls for enhanced security measures and industry-wide standardisation to safeguard operators and consumers alike.

Recent incidents have highlighted the potential misuse of AI in this sector. Over the Easter weekend, Sky News revealed an AI-generated video falsely portraying its presenters endorsing gambling apps. The video featured manipulated footage of news presenter Matt Barbet, discussing a fictitious win on an iPhone game. These deepfake adverts were disseminated via social media to promote illegal gambling sites within Apple’s App Store, raising concerns about AI's role in deceptive promotional content.

In response to these evolving threats, the UK’s Gambling Commission issued an update in April warning about AI deepfakes' prevalence and their connection to emerging money laundering and terrorist financing risks. Last year, the UK’s Joint Money Laundering Intelligence Taskforce issued an amber alert regarding AI's use to circumvent customer due diligence processes. Additionally, the National Crime Agency (NCA) dismantled a website selling AI-generated identity documents, such as passports and driver licences, at low cost. Consequently, the Gambling Commission has stressed the importance of training staff to recognise AI-generated documents effectively.

Dr Michaela MacDonald, senior lecturer in law and technology at Queen Mary University of London, explained that synthetic identity theft merges genuine and fabricated personal information to create entirely new fake identities. She told iGB, “Alongside voice cloning, behavioural mimicry, and deepfake technologies, AI-generated synthetic identities can easily bypass traditional Know Your Customer (KYC) systems by defeating facial recognition, exploiting support chats, or spoofing voice-activated authentication.” This highlights the ability of AI to evade conventional verification methods.

Research published by the Alan Turing Institute in March details how AI-enabled crime capitalises on the technology’s capacity to automate and scale up criminal activities. The report states, “UK law enforcement is not adequately equipped to prevent, disrupt or investigate AI-enabled crime.” It recommends a more robust approach featuring the proactive deployment of AI by law enforcement agencies.

Regulatory responses to such threats tend to be stringent, particularly regarding anti-money laundering (AML) breaches. In April, the Gambling Commission imposed penalties on two operators for AML failures. The Football Pools was fined £375,000 (€449,732/$484,417) for inadequate hard stop processes when AML thresholds were reached, while Corbett Bookmakers received a £686,070 fine for insufficient risk-based AML approaches. The Commission emphasised that operators must train staff to assess AI-generated documents proficiently.

Annabelle Richard, a legal partner at Pinsent Masons, cautioned that while regulators might initially be lenient towards AML rule breaches involving deepfakes—especially when operators are uncertain how to respond—failure to engage with authorities or update procedures could attract harsher penalties. “If you haven’t even engaged with the authority to say: ‘I’m not sure what I can and can’t do,’ it will be considered that you didn’t do what you were supposed to,” she said.

With fraud identified as the most prevalent crime in the UK, the NCA has raised concerns over AI's potential to amplify the scale and sophistication of scams. Deepfake images and videos complicate fraud detection and enable offenders to target a broader range of victims across language and geographical boundaries. The NCA stated to iGB, “The use of AI to facilitate fraud underscores the need for private industries, law enforcement and the public to all take steps to reduce the threat. The UK’s Online Safety Act puts more onus on the online platforms to take action, and we are continuing to work with government and regulators to maximise its impact.”

The 2023 UK Online Safety Act introduced measures requiring service providers to enhance account verification and deploy automated software to detect advertisements or posts linked to stolen or forged credentials. Such legislative steps aim to reduce the proliferation of fraudulent activities enabled by AI.

Operators are encouraged to refresh AML processes continuously to counter AI threats. Combining AI-based document verification with biometric technologies, including facial recognition and liveness detection, can improve fraud detection. The integration of device fingerprinting and geolocation further strengthens security measures. Dr MacDonald highlighted emerging technologies that centralise verification and employ machine learning to identify subtle inconsistencies and evolving fraud patterns rapidly and accurately.

Despite these tools, the gambling industry remains engaged in a continual contest with fraudsters. Mick d’Ancona, gambling sector expert and consultant at Circle Squared, noted to iGB that forged documentation has long been a challenge for operators. “All that’s happening now is it’s easier to [fake documents required by operators]. But actually, if you’re a good operator and you’ve been [processing documents] properly, you’ve got what you need in place,” he said. At the same time, d’Ancona warned smaller operators or those in less regulated markets could be more exposed to due diligence failures due to budget limitations or less rigorous processes.

One promising development to mitigate identity fraud is the implementation of national digital identity wallets. These utilise cryptographic keys and biometric verification to provide secure digital identification. Countries such as Singapore and Estonia pioneered such systems in 2002. Other nations including Germany, Sweden, Japan, Canada, and the UK have introduced or are advancing digital ID solutions. The EU's Digital Identity Framework Regulation, effective in 2024, mandates member states to offer digital identity wallets, facilitating secure identification for public and private services.

Jarek Sygitowicz, co-founder of Authologic, a developer of identity verification software, expressed optimism about electronic ID wallets. Speaking to iGB, he said, “These have seen adoption growing over the years, but with the EU implementing the eIDAS 2.0 regulation, what has been a slow wave will become a big jump in the next 12-24 months.”

Despite the availability of advanced tools, the industry currently lacks consistency in addressing AI-driven fraud. Peter Wood, CTO of Web3 recruiter Spectrum Search, emphasised the need for shared frameworks and enhanced collaboration among platforms. He stated, “Regulators should be pushing for industry-wide standards around ID verification that are designed to hold up against AI. We also need to see better collaboration between platforms, some kind of anonymised, real-time data sharing system that helps flag suspicious activity across the board.”

Fragmentation of personal data across multiple platforms complicates synthetic identity fraud detection. Dr MacDonald recommended international coordination for synthetic ID detection, information sharing, and regulatory standard-setting to keep pace with increasingly sophisticated AI-enabled fraud.

In conclusion, while the risks posed by AI in the gambling sector are accelerating, technological countermeasures and regulatory frameworks are evolving correspondingly. Maintaining updated knowledge, investing in robust verification technologies, and fostering cooperation between regulators and operators remain central to managing these emerging challenges.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://igamingbusiness.com/tech-innovation/artificial-intelligence/how-much-of-a-threat-ai-are-deepfakes-to-the-gambling-sector/> - Corroborates the threat of AI-enabled fraud and deepfakes in the gambling sector, including incidents like AI-generated videos promoting illegal gambling sites. It highlights the need for operators to enhance security measures to mitigate these risks.
2. <https://www.biometricupdate.com/202501/surge-of-online-gambling-fraud-pushing-industry-towards-identity-verification-report> - Supports the growth of the gambling industry alongside an increase in fraud, emphasizing the role of AI in real-time fraud detection and identity verification.
3. <https://iagr.org/industry-news/leveraging-ai-to-protect-people-who-gamble/> - Discusses how AI is used in the gambling industry to detect fraud and improve player safety, while also raising ethical concerns about AI's potential impact on gambling behaviors.
4. <https://www.gamblingiq.co.uk/post/igaming-s-evolving-threats-deepfakes-bonus-abuse-and-security-innovations-featuring-leading-anti> - Highlights the evolving threats such as deepfakes, bonus abuse, and the need for AI-powered verification to combat fraud in the gambling industry.
5. <https://www.socure.com/blog/first-party-fraud-online-gaming-industry-losses> - Details the significant financial losses due to fraud in the online gaming industry, which necessitates more robust security and verification measures.
6. <https://www.noahwire.com/> - Though not specifically related to the above content, it serves as a news source that could potentially cover topics related to AI, fraud, and gambling. However, for direct corroboration of the article’s claims, it lacks specific relevance without additional context.
7. <https://news.google.com/rss/articles/CBMiyAFBVV95cUxQeC1LS1hteEVBZTBfVlpYWGxZV1dhMlRVeFdOb0EzZEFaRjBmZ043cTc4TUc4UzZOZWw1bkoxTzJCSmhkM0llQ1A0OGpXX2llYmc1VkRkNEZ0cXQ1RTFGVjRCaFU5OHlJRlZZM0NWVzI0NjF3dzNBYTh6N3pGdzNiS2FkV2FjVHNCenJUSDhJZUZMb1A1Y0dzc0NDb3VyOWtvb2RwOU9FY2tFQWgwZXFyQkc5SXBsMThDZmQxLUpwLW1xVHo4SllTdg?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data