# Finance director loses $25 million in deepfake scam as blockchain emerges as key defence



In January 2024, the finance director of a UK firm fell victim to a highly sophisticated scam, transferring $25 million to fraudsters after a video call with what seemed to be the company's CFO. This scenario epitomises a growing trend in cybercrime, driven by advancements in deepfake technology, which has become alarmingly sophisticated. Such incidents are not rare; they exemplify a broader challenge, as global losses resulting from eCommerce fraud are projected to soar from $44 billion in 2024 to an eye-watering $107 billion by 2029, marking a staggering 141% increase according to a report from Juniper Research.

The implications of these developments extend beyond immediate financial losses. A significant 60% of consumers now express scepticism about the authenticity of online content, attributing their concerns to AI-generated misinformation and deepfake technology. This reality is underscored by findings from Accenture's Life Trends 2025 report, which highlight the shifting landscape of trust and authenticity in consumer interactions.

For entrepreneurs and business leaders, the dual threats of reputational harm from deceptive media and potential legal ramifications loom large as governments worldwide introduce stringent AI disclosure regulations. Current measures, such as watermarking and AI detection tools, tend to be reactive. Watermarking can be easily manipulated, while detection systems reportedly fail to identify altered content nearly 30% of the time, as researchers from the University of Pennsylvania have uncovered. Legal recourse often comes too late to contain the damage.

In tackling this issue, a promising solution has emerged: the integration of blockchain technology with AI-powered digital twins. These digital avatars serve as a bridge between the physical and digital realms, capable of optimising systems across various sectors—from healthcare to retail. By assigning AI avatars with NFT passports—tamper-proof digital certificates stored on a blockchain—businesses can establish a verifiable record of the avatar's origin and changes, thereby enabling preemptive measures against fraud.

Recent trends suggest that consumer trust is heavily reliant on transparency. A 2024 Edelman report indicates that 62% of consumers would only trust AI-generated content if its provenance was verifiable. Blockchain-based authentication effectively addresses this demand. Sectors from luxury goods to healthcare are already adopting this model. For instance, Swiss watchmaker Breitling has collaborated with Arianee to integrate blockchain-based digital passports for its timepieces. Similarly, the UK's National Health Service has initiated blockchain technology to authenticate medical professionals amid rising impersonation scams.

Navigating the evolving landscape of AI requires a proactive strategy for entrepreneurs. Public figures are particularly vulnerable to deepfake manipulation, necessitating vigilant monitoring for fraudulent materials. Businesses should anchor their digital identities in verifiable technologies like blockchain and remain attuned to regulatory changes such as the forthcoming EU AI Act, which imposes severe penalties for undisclosed synthetic media. Such regulations reflect a global shift towards stricter oversight of AI technologies.

Moreover, prioritising digital identity protection should be approached with the same diligence as cybersecurity. Assigning accountability, conducting regular audits of AI tools, and exploring partnerships with insurers specialising in deepfake liability can bolster an organisation’s resilience against these burgeoning threats.

As deepfake fraud evolves from a theoretical risk to a pressing reality, the need for proactive and robust authentication measures has never been more critical. While detection tools hold utility, integrating blockchain technology to secure identity and authenticity offers a powerful line of defence. The path forward is clear: businesses must choose to invest in verification now or face the potential fallout of synthetic scams in the future. In this accelerating era of AI technology, authenticity will not merely be advantageous; it will underpin the trust and competitive edge necessary for success.

**Reference Map**

1. Paragraph 1: [[1]](https://www.entrepreneur.com/science-technology/how-to-protect-your-business-from-deepfake-fraud/491362), [[2]](https://www.ft.com/content/b977e8d4-664c-4ae4-8a8e-eb93bdf785ea), [[4]](https://www.theverge.com/2024/2/5/22267456/hong-kong-deepfake-video-conference-employee-transfer-25-million), [[5]](https://www.scmagazine.com/news/deepfake-video-conference-convinces-employee-to-send-25m-to-scammers)
2. Paragraph 2: [[1]](https://www.entrepreneur.com/science-technology/how-to-protect-your-business-from-deepfake-fraud/491362), [[3]](https://www.globenewswire.com/news-release/2024/10/07/2958648/0/en/eCommerce-Fraud-to-Exceed-107-Billion-in-2029.html)
3. Paragraph 3: [[1]](https://www.entrepreneur.com/science-technology/how-to-protect-your-business-from-deepfake-fraud/491362), [[2]](https://www.ft.com/content/b977e8d4-664c-4ae4-8a8e-eb93bdf785ea)
4. Paragraph 4: [[1]](https://www.entrepreneur.com/science-technology/how-to-protect-your-business-from-deepfake-fraud/491362), [[2]](https://www.ft.com/content/b977e8d4-664c-4ae4-8a8e-eb93bdf785ea)
5. Paragraph 5: [[1]](https://www.entrepreneur.com/science-technology/how-to-protect-your-business-from-deepfake-fraud/491362), [[4]](https://www.theverge.com/2024/2/5/22267456/hong-kong-deepfake-video-conference-employee-transfer-25-million)
6. Paragraph 6: [[1]](https://www.entrepreneur.com/science-technology/how-to-protect-your-business-from-deepfake-fraud/491362), [[3]](https://www.globenewswire.com/news-release/2024/10/07/2958648/0/en/eCommerce-Fraud-to-Exceed-107-Billion-in-2029.html), [[7]](https://www.businessamlive.com/global-ecommerce-risks-107bn-devastation-by-2029-over-rising-ai-powered-fraud/)
7. Paragraph 7: [[1]](https://www.entrepreneur.com/science-technology/how-to-protect-your-business-from-deepfake-fraud/491362), [[3]](https://www.globenewswire.com/news-release/2024/10/07/2958648/0/en/eCommerce-Fraud-to-Exceed-107-Billion-in-2029.html)
8. Paragraph 8: [[1]](https://www.entrepreneur.com/science-technology/how-to-protect-your-business-from-deepfake-fraud/491362), [[4]](https://www.theverge.com/2024/2/5/22267456/hong-kong-deepfake-video-conference-employee-transfer-25-million)

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

## Bibliography

1. <https://www.entrepreneur.com/science-technology/how-to-protect-your-business-from-deepfake-fraud/491362> - Please view link - unable to able to access data
2. <https://www.ft.com/content/b977e8d4-664c-4ae4-8a8e-eb93bdf785ea> - In May 2024, UK engineering firm Arup lost HK$200 million (approximately $25 million) due to a sophisticated deepfake scam. Fraudsters used a digitally cloned version of a senior manager during a video conference to authorize financial transfers. This incident underscores the growing threat of deepfakes in cybercrime, highlighting the need for enhanced cybersecurity measures. Arup reported the fraud to Hong Kong police in January, stating that its financial stability and operations were unaffected. The case led to the resignation of Arup's East Asia chair, Andy Lee, and emphasizes the importance of vigilance against such scams.
3. <https://www.globenewswire.com/news-release/2024/10/07/2958648/0/en/eCommerce-Fraud-to-Exceed-107-Billion-in-2029.html> - A study by Juniper Research predicts that eCommerce fraud will increase from $44 billion in 2024 to $107 billion in 2029, marking a 141% rise. The report highlights that AI is enabling fraudsters to execute more sophisticated attacks, including the use of deepfakes to bypass verification systems. It emphasizes the necessity for eCommerce merchants to integrate AI-driven fraud prevention systems to swiftly identify emerging fraudulent tactics, particularly in developed markets where larger merchants are more susceptible to such threats.
4. <https://www.theverge.com/2024/2/5/22267456/hong-kong-deepfake-video-conference-employee-transfer-25-million> - In February 2024, a Hong Kong employee was deceived into transferring $25 million to scammers after participating in a video conference with what appeared to be the company's CFO. The fraudsters used AI-generated deepfake technology to create convincing video and audio, leading the employee to believe the request was legitimate. This incident highlights the increasing sophistication of cybercriminals using deepfakes to manipulate individuals into unauthorized financial transactions, underscoring the need for enhanced security measures and employee training to recognize such scams.
5. <https://www.scmagazine.com/news/deepfake-video-conference-convinces-employee-to-send-25m-to-scammers> - In February 2024, a deepfake phishing scam resulted in a multinational company losing over $25 million. An employee was tricked into transferring funds after a video conference with AI-generated imitations of colleagues. The fraudsters initially contacted the employee via email, posing as the company's UK-based CFO. After a convincing video call, the employee transferred $200 million HKD (approximately $25.6 million USD) to five different bank accounts across 15 transactions. The scam was discovered a week later when the employee contacted the company's headquarters directly. This case underscores the need for businesses to update security training and implement multi-level approval processes for financial transactions.
6. <https://www.businesswire.com/news/home/20220710005013/en/Juniper-Research-Online-Payment-Fraud-Losses-to-Exceed-343-Billion-Globally-Over-the-Next-5-Years-Juniper-Research-Study-Finds> - Juniper Research forecasts that cumulative merchant losses to online payment fraud globally between 2023 and 2027 will exceed $343 billion. This projection highlights the massive scale of online payment fraud and the urgent need for enhanced fraud prevention measures. The study emphasizes the importance of integrating advanced verification tools at critical points in the customer journey to effectively protect users and mitigate losses. The findings underscore the necessity for businesses to adopt comprehensive fraud prevention strategies to safeguard against evolving cyber threats.
7. <https://www.businessamlive.com/global-ecommerce-risks-107bn-devastation-by-2029-over-rising-ai-powered-fraud/> - Juniper Research warns that global eCommerce is at risk of losing $107 billion by 2029 due to rising AI-powered fraud. The report highlights that AI is enabling fraudsters to execute more sophisticated attacks, including the use of deepfakes to bypass verification systems. It also notes a growing trend of 'friendly fraud,' where customers themselves commit fraud, such as refund fraud. The study emphasizes the need for eCommerce merchants to integrate AI capabilities into fraud prevention systems to quickly identify emerging tactics and protect their businesses from increasingly sophisticated cyber threats.