# Network exploits deepfake technology to scam millions from victims across the globe



An organised network operating from Georgia has orchestrated a significant scam that has defrauded victims in the UK, Europe, and Canada of approximately $35 million (£27 million) by leveraging deepfake technology and false celebrity endorsements on social media platforms, notably Facebook and Google. The fraudulent operation has reportedly claimed thousands of savers, with UK citizens suffering the most significant losses.

The scam employed convincing deepfake videos that featured well-known figures such as money expert Martin Lewis, radio DJ Zoe Ball, and adventurer Ben Fogle, promoting fictitious cryptocurrency schemes and dubious investment opportunities. The perpetrators, who are believed to still be reaching out to potential victims, ran their operations out of three office blocks in Tbilisi, Georgia, under the moniker "skameri," which translates to scammers in Georgian.

The extent of the deception was brought to light through a major data leak of scam call centre records, which was shared with various international media outlets, including The Guardian, by the Swedish public broadcaster SVT. This leak revealed over one million recordings, including conversations with victims who lost substantial sums of money. According to the records, around 6,000 individuals worldwide fell victim to this fraudulent scheme since May 2022, with nearly half of the calls directed at UK numbers.

Notably, UK victims accounted for about £9 million of the total losses. The data indicated that 652 of the highest loss victims, who collectively surrendered large amounts of their savings, hailed from the UK. One victim, a former NHS doctor in her 70s from London, reportedly lost around £50,000 after spending over 55 hours communicating with the scammers. Tragically, it is believed that she passed away shortly after her last interaction with the call centre. Another victim, a retired employee of the London Stock Exchange, spent more than 135 hours speaking to the fraudsters and lost £162,000.

The fraudulent advertisements, which frequently referenced tech billionaire Elon Musk, were allegedly placed by affiliate marketers who operated anonymously while collecting contact information of potential targets. The data leaked has drawn attention to the lavish lifestyle indulged in by the scammers, who spent their ill-gotten gains on luxury items such as Rolex watches and extravagant parties.

The rise of Authorised Push Payment (APP) fraud, where victims are tricked into sending money directly from their accounts, has been alarming, with reports indicating a 12% increase in such cases to over 230,000 incidents in 2023, according to UK Finance.

Despite the UK government enacting a new set of laws intended to protect citizens online, gaps remain in the implementation, particularly concerning fraudulent advertising. The Online Safety Act has been passed, but its provisions addressing misleading ads by corporations are not expected to take effect until next year.

Commenting on the situation, Chi Onwurah, the chair of the Commons Science, Innovation and Technology Committee, highlighted the urgency of ensuring the Online Safety Act can effectively safeguard the public and tackle current challenges posed by misinformation and online scams. The government reiterated that such scams are a criminal offense and stressed that social media platforms must assume responsibility for preventing their sites from facilitating fraud.

In response to the ongoing issues, spokespeople from various affected companies have pledged to fight against such scams rigorously. A representative from Revolut noted that 60% of reported scams among their UK customer base in 2023 originated from platforms owned by Meta, the parent company of Facebook. Meanwhile, Meta asserted its commitment to combatting scams, emphasising cooperative measures such as its Fraud Intelligence Reciprocal Exchange (FIRE) programme.

As investigations continue and awareness of online fraud rises, the complex interplay between technology, celebrity endorsements, and safeguarding consumer interests remains a focal point of discourse among regulators and the public alike.

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

## References

* <https://www.trendmicro.com/vinfo/mx/security/news/cyber-attacks/unusual-ceo-fraud-via-deepfake-audio-steals-us-243-000-from-u-k-company> - This article highlights the use of deepfake technology in fraud, similar to the scam described in the article, where deepfake videos were used to deceive victims. It shows how AI-generated content can be used for financial scams.
* <https://www.aiaaic.org/aiaaic-repository/ai-algorithmic-and-automation-incidents/dubai-usd-35m-voice-cloning-fraud> - This incident involves deepfake voice cloning used to defraud a company, illustrating the sophisticated methods scammers use, similar to the deepfake videos in the article.
* <https://securityaffairs.com/158651/cyber-crime/cyber-heist-with-deepfake-tech.html> - This article discusses a scam involving deepfake video calls, which is similar to the deepfake videos used in the scam described in the article to deceive victims.
* <https://www.theguardian.com/technology/2023/sep/14/online-safety-bill-misleading-ads> - This article discusses the challenges posed by misleading ads online and the need for stronger regulations, aligning with the article's mention of gaps in the implementation of laws addressing fraudulent advertising.
* <https://www.ukfinance.org.uk/press/press-releases/authorised-push-payment-fraud-increases-12-2023> - This report from UK Finance highlights the rise in Authorised Push Payment (APP) fraud, which is relevant to the article's discussion on the increase in such scams.