# Organised fraud network scams UK and global savers out of £27 million



An organised network based in Georgia has defrauded savers across the UK, Europe, and Canada out of approximately $35 million (£27 million) through elaborate scams facilitated by fake celebrity endorsements on social media platforms like Facebook and Google. The fraudulent operation, which employs sophisticated deepfake technology and misleading news reports, has exploited the names of well-known figures, including financial expert Martin Lewis, radio presenter Zoe Ball, and adventurer Ben Fogle, to lure victims into investing in non-existent cryptocurrency schemes.

As revealed in a recent data leak, which involved over one million call records shared with Swedish public broadcaster SVT and the Organized Crime and Corruption Reporting Project (OCCRP), these scams have continued unabated, with reports suggesting that scammers were still reaching out to victims in recent weeks. The leak has provided a rare glimpse into the mechanisms behind the fraud, including detailed accounts of conversations between scammers and their victims, detailing the emotional and financial toll on individuals.

UK citizens were particularly affected, accounting for about a third of the total losses, approximately £9 million. Victims included pensioners, employees, and small business owners, with around 6,000 individuals worldwide fallen prey to this fraud since mid-2022. Notably, a former NHS doctor in her 70s lost around £50,000 following prolonged conversations with the scammers, during which she expressed her desperation, stating, “I’ve used up every penny of my savings, I have nothing. And I can’t survive like that.” Tragically, she is believed to have died shortly after her last contact with the call centre. Another victim, a retired employee of the London Stock Exchange, spent over 135 hours in conversation with the fraudsters and lost more than £162,000.

According to the leaked records, the scammers referred to themselves as the "skameri," operating out of three office blocks in Tbilisi. They targeted victims by employing affiliate marketers who placed deceptive ads in exchange for a percentage of the profits. The data suggests that they had a significant focus on UK residents, with 45% of their calls directed to UK numbers.

The UK government has been working on legislation aimed at combating such threats, including the Online Safety Act. While this act, which aims to enhance online protection for children and adults, has been passed into law, enforcement provisions regarding fraudulent advertising are not slated to take effect until next year. Amidst this legislative backdrop, instances of authorised push payment (APP) fraud have reportedly risen by 12%, leading to over 230,000 cases in 2023, according to UK Finance.

In response to these incidents, financial institutions like Revolut, Kroo, and Chase, which have been linked to the scams as channels for processing payments, expressed their commitment to combatting fraud. A spokesperson from Revolut noted that a significant portion of reported scam cases involved customers who had originally been targeted through Meta platforms like Facebook and WhatsApp.

Martin Lewis, Zoe Ball, and Ben Fogle have previously condemned the use of deepfake technology in fraudulent adverts. Lewis notably took legal action against Facebook in 2018 over the issue, though he later dropped the suit after the platform agreed to fund an anti-scam initiative. In recent statements, MP Chi Onwurah highlighted the pressing need for effective measures within the Online Safety Act to address online misinformation and frauds, while a government spokesperson underlined the importance of social media platforms’ responsibility in preventing scams.

Meta has claimed adherence to company policies prohibiting scam-related ads and has called for collaborative efforts to tackle these frauds, while Google maintains that user protection is its top priority and strictly enforces its advertising policies against scams. As this issue continues to unfold, the impact on victims and the effectiveness of legislative and corporate responses remain to be seen.

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

## References

* <https://www.noahwire.com> - This URL is the source of the article detailing the organized network based in Georgia that has defrauded savers across the UK, Europe, and Canada through elaborate scams facilitated by fake celebrity endorsements.
* <https://www.svt.se/> - This URL is related to the Swedish public broadcaster SVT, which received over one million call records as part of a data leak revealing the mechanisms behind the fraud.
* <https://www.occrp.org/> - This URL is for the Organized Crime and Corruption Reporting Project (OCCRP), which collaborated with SVT on the data leak exposing the fraud operation.
* <https://www.gov.uk/government/news/online-safety-bill> - This URL provides information about the UK's Online Safety Act, aimed at enhancing online protection and combating fraudulent advertising.
* <https://www.meta.com/policies/ads/> - This URL outlines Meta's advertising policies, which prohibit scam-related ads, as mentioned in the article.