# Cloning scams reach record £2.7 million losses as AI boosts fraud sophistication



Consumers are facing an alarming increase in cloning scams, a sophisticated form of fraud that has garnered significant attention from industry experts and regulatory bodies. According to a recent report from the Investment Association, fraudsters lifted £2.7 million from customers of legitimate investment firms in the latter half of 2024 alone. These scams involve creating nearly identical copies of legitimate companies' websites, emails, or even fake WhatsApp groups to mislead consumers into sending payments. The findings highlight that impersonation scams are now a top threat for consumers wanting to invest.

The report, released to coincide with “Take Five” fraud prevention week, revealed 478 instances of impersonation related to investment management companies during this time, with nearly one in four attempts being successful. Adrian Hood, a regulatory and financial crime expert at the Investment Association, emphasised that fraudsters employ a variety of tactics, from impersonating investment managers to stealing card details or illicitly accessing accounts.

The rise of artificial intelligence technology has notably escalated the sophistication of these scams. Hood warned that AI tools enable criminals to mimic legitimate firms with greater efficacy. This concern is echoed by other financial bodies, with the National Crime Agency reporting that over £78 million was lost to "clone firm" investment scams in 2020 alone. Consumers are urged to verify investment opportunities through the Financial Conduct Authority's (FCA) register, ensuring they only deal with registered firms.

Despite the troubling trends, there are signs of progress in the battle against fraud. The Investment Association also noted that overall fraud losses for consumers fell by 29%, down to £5.4 million, between the first and second halves of the year. Furthermore, efforts to counter account takeovers have shown results, with a drop in reported cases from 142 to 132.

The Financial Services Compensation Scheme has raised alarms about the ongoing increase in online financial scams, particularly those involving brand cloning. Many of these scams target hopeful investors through misleading online advertisements and fake price-comparison websites. In the same vein, a report from the Global Anti-Scam Alliance revealed that UK consumers lost £11.4 billion to various scams over the past year—an increase of £4 billion from the previous year.

In light of these findings, UK Finance has cautioned consumers to remain vigilant, suggesting they carefully check the authenticity of email addresses and websites, looking for subtle discrepancies that could indicate fraud. They advise confirming any firm’s legitimacy through the FCA’s register before engaging financially. Immediate reporting to local police and the Action Fraud centre is recommended for anyone who suspects they have fallen victim to a cloning scam.

The landscape of financial scams is evolving at a rapid pace, necessitating both increased public awareness and proactive measures from regulatory bodies to protect consumers. As technology continues to advance, so too do the methods employed by scammers, making ongoing vigilance essential in safeguarding personal and financial information.

### Reference Map

1. Paragraph 1: Sources (1), (2)
2. Paragraph 2: Sources (1), (2)
3. Paragraph 3: Sources (2), (3), (4)
4. Paragraph 4: Sources (2)
5. Paragraph 5: Sources (5), (6)
6. Paragraph 6: Sources (2), (3)
7. Paragraph 7: Sources (2), (6)

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

## Bibliography

1. <https://www.ft.com/content/4aea4a81-10d5-48f2-8594-8883a298363f> - Please view link - unable to able to access data
2. <https://www.ft.com/content/4aea4a81-10d5-48f2-8594-8883a298363f> - Consumers have been warned to remain on the lookout for so-called cloning scams after a UK investment trade body found fraudsters took £2.7mn from members’ customers through the practice in the second half of 2024. Criminals perpetrating the scams create a nearly identical duplicate of a legitimate company’s website, email or a fake WhatsApp group to persuade consumers to send them payments. Such frauds were “topping the list of threats” facing consumers who wanted to invest, a report by the Investment Association found. The study was published to mark “Take Five” fraud prevention week. There were 478 reports of impersonation of investment management companies in the second half of 2024, according to the report. Just under one in four was successful. Adrian Hood, a regulatory and financial crime expert at the association, said criminals would use “a variety of means” to trick people into parting with their money. They could impersonate genuine investment managers, steal card details or fraudulently log into a person’s account. The IA advised consumers to “stay vigilant”, double-checking senders’ email addresses and web addresses for slight differences from those of legitimate companies. Hood said the risk was growing more acute as fraudsters used new artificial intelligence (AI) technology. “The growth of AI is likely to see increasingly sophisticated scams, with criminals better able to mimic legitimate firms,” he said. There were 1,014 cloning scams against IA member firms detected in 2024, a 57 per cent increase on the year before, despite an overall fall in the number of other scams detected. However, the association said efforts to counter fraud generally were succeeding, and that losses from fraud for its members’ customers fell by 29 per cent, to £5.4mn, between the first and second halves of 2024. Some £1.7mn scammed from members’ customers was recovered. There was a drop in the number of account takeovers, in which fraudsters take control of an account to cash in an investment, from 142 to 132 between the two halves of the year. Over the same period, there was a decline in reports of card fraud, in which a criminal uses stolen card details to open an investment account, from 36 to 17. UK Finance said criminals already went to great lengths to appear legitimate and AI tools could make it easier for them to do so. “People can check the Financial Conduct Authority’s register for lists of regulated firms and only use the contact details listed on the register to confirm you’re dealing with the genuine firm before parting with your money or information,” it said. Customers who believe they have been scammed are advised to contact their investment platform or provider immediately and report the incident to UK police forces’ Action Fraud centre.
3. <https://www.actionfraud.police.uk/news/clonefirms> - Action Fraud, the City of London Police, and the Financial Conduct Authority (FCA) have issued a warning about the rise in 'clone firm' investment scams. These scams involve fraudsters setting up fake firms using the name, address, and Firm Reference Number (FRN) of real companies authorized by the FCA. Victims are often targeted through online advertisements and false price-comparison websites, leading them to believe they are dealing with legitimate investment firms. In 2020, over £78 million was lost to these scams, with victims losing an average of £45,242 each. The FCA advises consumers to verify investment opportunities by checking the FCA Register and to use contact details listed there to ensure they are dealing with genuine firms.
4. <https://www.nationalcrimeagency.gov.uk/news/over-78-million-stolen-in-clone-firm-investment-scams/> - The National Crime Agency (NCA) has reported that over £78 million was stolen in 'clone firm' investment scams. Fraudsters set up fake firms using the name, address, and Firm Reference Number (FRN) of real companies authorized by the Financial Conduct Authority (FCA). These scams often involve sending sales materials linking to websites of legitimate firms to deceive potential investors. The FCA advises consumers to check the Warning List of firms and to only deal with firms authorized by the FCA. Specific details of a firm, such as telephone numbers and website addresses, can be verified on the FCA Register.
5. <https://www.fscs.org.uk/news/fraud/worrying-rise-in-online-financial-scams/> - The Financial Services Compensation Scheme (FSCS) has highlighted a worrying rise in online financial scams, particularly 'brand cloning' scams. In these scams, criminals clone well-known financial services brands to produce fake adverts, documents, and websites. They use targeted online adverts and false price-comparison websites to reach people searching for products such as pensions and ISAs. This tricks people into following false links and ultimately transferring their money to scammers. In 2020, more than £78 million was lost to brand cloning scams, with victims losing an average of £45,242 each. The FCA issued more than 1,000 scam warnings in 2020, 40% of which involved clones or impersonations of legitimate financial services brands.
6. <https://www.cifas.org.uk/newsroom/gasa-stateofscamsuk2024> - The Global Anti-Scam Alliance’s (GASA) latest report, The State of Scams in the UK, conducted in association with Cifas, revealed that UK consumers lost £11.4 billion to scams in the last 12 months, up £4 billion from the previous year. The report highlights that 15% of consumers surveyed had lost money to criminals in 2024, with an average loss of £1,400 per victim. The most common scams included rogue delivery messages, shopping, and investment scams. The report also noted that 71% of victims did not report the scams to the police or law enforcement. The findings underscore the need for increased awareness and vigilance among consumers to protect themselves from evolving scam tactics.
7. <https://www.itv.com/news/2024-09-17/ai-voice-cloning-scam-warning-issued-by-bank> - Starling Bank has issued a warning about the rise of AI voice cloning scams, where fraudsters use artificial intelligence to replicate a person’s voice from just a few seconds of audio. Scammers can then use the cloned voice to contact family members and friends, asking for money urgently. A survey for the bank found that nearly half (46%) of people did not know this type of scam existed, and 8% said they would be likely to send money if they received such a call, even if it seemed strange. The bank advises consumers to be aware of this emerging scam and to use safe phrases with close friends and family to verify the authenticity of such calls.