Global Counsel

# The new "Scamdemic" – how is the UK government tackling emerging financial scams?

**Blog post by Associate Leanne Gaffney-Berkeley, 17 November 2021**

The covid-19 pandemic has seen a rapid rise in new and sophisticated types of financial scams in the UK, typically targeting ordinary consumers. People are more likely to be the victim of financial fraud than of any other crime – not just including the vulnerable and elderly – with more than two thirds of people in the UK (36 million) being targeted by a scammer in the first half of this year, resulting in £753.9 million lost through fraud, representing an increase of 30% compared to the same time last year.

Authorised push payment (APP) scams - where a victim transfers money into the bank account of a criminal under the impression they are a trusted organisation such as a bank or utility company – grew fastest during the pandemic. Total losses due to these scams increased to £355.3 million in the first half of 2021, up 71% compared to the same period in 2020. Purchase scams accounted for almost half of all APP cases.

For financial institutions and other service providers the surge in fraudulent activity is already a major practical challenge. It erodes trust in consumer communications and tests their fraud alert mechanisms. In many cases new security measures introduced can increase bureaucracy and transactional friction for consumers, which in turn impacts customer satisfaction and can damage brands. At the same time as they rush to address these new challenges, it seems likely that they will also need to engage with government and regulators who also want to be seen to be taking action.

Significantly, many of the new scams fly under the radar of the government's previous plans to tackle financial fraud. Nor are they necessarily addressed by current rules. Under current UK legislation if a customer authorises a fraudulent payment, whilst they may be partly or wholly compensated at the discretion of their bank, they have no legal protection to cover them for losses. This burst of criminal activity and consumer losses suggests that we can expect to see a response from government and regulators. But what might this mean in practice?

There have been strong calls for a more comprehensive approach. Since the start of this year we have seen the Home Office and multiple sectoral regulators including Ofcom, the Financial Conduct Authority (FCA) and Pensions Regulator seeking to work together on new initiatives to tackle financial fraud by bringing together impacted sectors – namely banks, telecom companies and tech firms. This is in part a response to the criticism that the 2019 Economic Crime plan focused too heavily on banks.

The UK government recently relaunched the Joint Fraud Taskforce, accompanied by new charters committing the retail banking, telecoms, and accountancy sectors to help close the vulnerabilities that criminals exploit to conduct fraud. Proposed initiatives include a pilot dynamic direct debit system to authenticate applications for new mobile phone contracts and leveraging new technology to tackle the fraudulent practice of sending fake company text messages – known as 'smishing'. Ofcom has also recently announced it is working with telecoms companies to block suspicious international calls at their source that are masked by a UK number.

There are also increasing calls from UK regulators, as well as industry, consumer bodies and charities for the government's draft Online Safety Bill to include types of online fraud which were excluded from it when it was published earlier in May. Currently the government's proposed legislation covers fraud linked to user-generated content but not fraud linked to paid-for advertising (such as investment and purchase scams). The FCA used its latest perimeter report to propose that the Bill should be expanded to include paid-for-advertising, where content relating to fraud would become 'priority' illegal content, thus requiring preventative action by platforms.

Seeing the direction Ofcom has taken with telecoms companies, we could expect the government will impose similar requirements on platforms to take down scam adverts in the Online Safety Bill.

There are a number of ways we may see the government act. The government could require platforms to collaborate together more to tackle scam adverts. Platforms don't currently share data with each other, as it could undermine their business models and because they claim this breaches user privacy rights. However, the government could call for platforms to share data and intelligence on known scammers in a bid to quickly block them across multiple platforms before they can target more victims.

The government may ask platforms to invest more in both human and AI review systems to identify, remove and block fraudulent online accounts and content. It could impose an obligation on all advertisers to be verified before their ads are published online, or on platforms to introduce clear and transparent labels for ads listed by unverified advertisers so consumers are aware of the risks. Some platforms have recently begun requiring advertisers to demonstrate they're authorised by the FCA, although in many cases the verification process can take up to a month, giving fraudsters ample time to target victims. The government may require platforms to rapidly verify all advertisers, including those not covered by the FCA.

The government may also require platforms to improve awareness among their users on how to recognise scams, encourage users to report fraudulent content and take more action to report cases to law enforcement. Currently, reporting by scam victims is low either because they don't know how to or they doubt any action will be taken by the platforms, and so platforms may need to give more confidence to users and demonstrate to the government that they take reporting seriously.

The challenge for the government and regulators will be ensuring platforms take proactive, meaningful action to address scam adverts and designing a scheme that can keep pace with the ever-changing nature of the threat. As technology and regulation evolves, so will the approach of criminals.