



Understanding Online Financial Harm

Financial Disinformation, Fraud and Exposure Across Demographic Groups in the UK

Evidence from a literature review

Benedetta Riciputi, Srividya Ivatury
22 Sept 2026

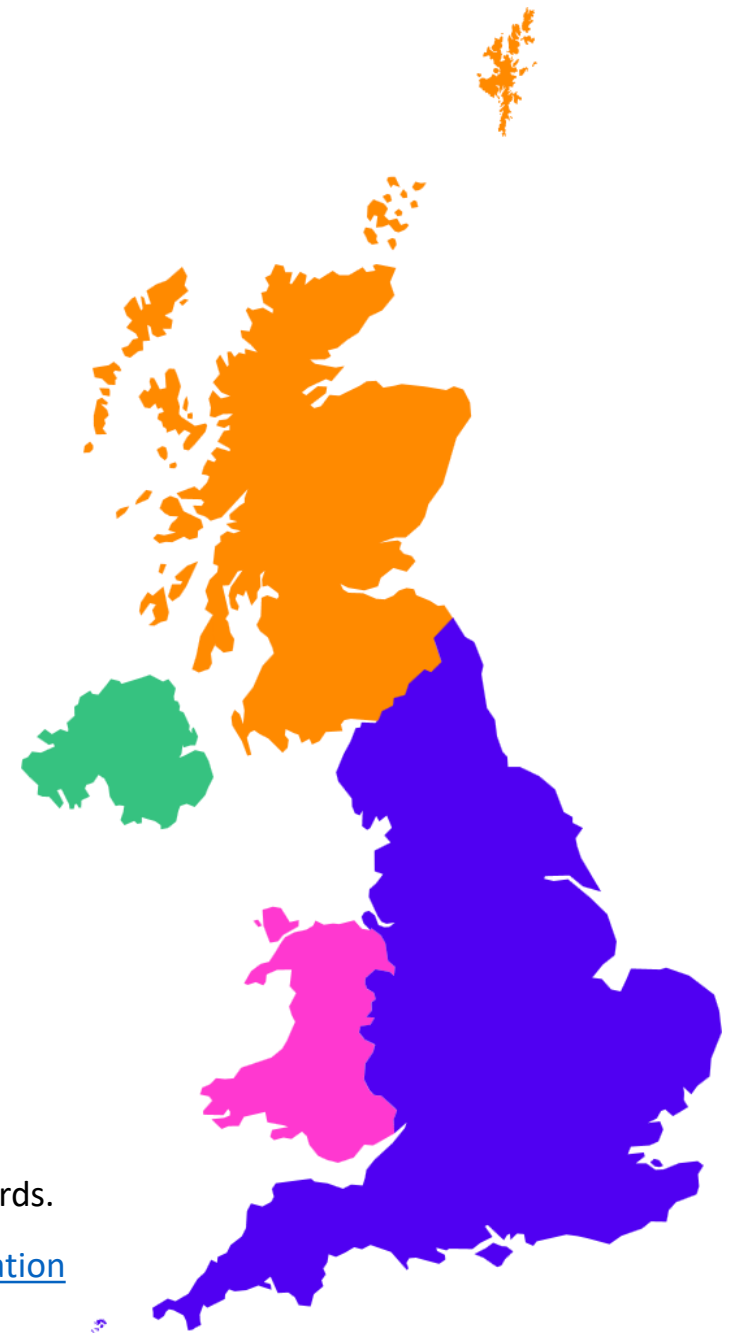
What this review looked at

This literature review examines how financial disinformation shared online can facilitate fraud, and understand the impact this has on victims across different demographic groups in the UK.

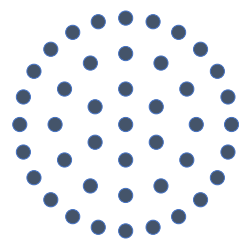
Focus: Financial disinformation deliberately designed to deceive, manipulate or defraud individuals, with financial harm as the immediate impact.

Evidence base: UK-relevant academic and grey literature, prioritising sources published from 2020 onwards.

Disclaimer: This presentation reflects the existing evidence and findings from the [Financial Disinformation](#) literature review. No new evidence, research, or findings have been added.

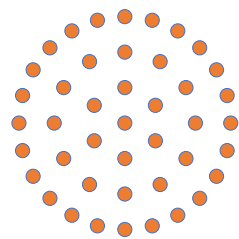


The scale of the problem



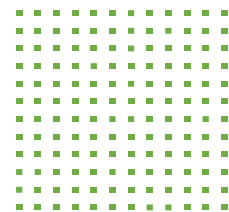
£6.8bn

Minimum societal cost of fraud against individuals



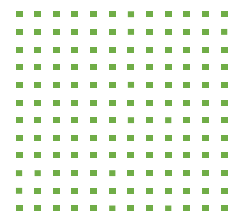
£4.2m

Estimated fraud incidents, year ending March 2025



41%

Of crime captured in the survey



67%

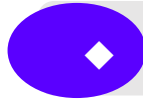
Of fraud reported in the UK estimated cyber-enabled

87% of UK adult internet users reported encountering suspected scam/fraud content; 46% said they had engaged with an online scam or fraud attempt.

How financial manipulation operates

Financial disinformation is a mechanism used across many fraud formats, including impersonation, investment scams, fake financial services, loan fee fraud, counterfeit websites, fraudulent advertising and fake jobs.

False legitimacy



Impersonating trusted people, organisations or services

Urgency



Pressuring people to act quickly

**Unrealistic
rewards**



Promising returns, prizes or opportunities

**Exploitation of
trust**



Combining false claims with real information

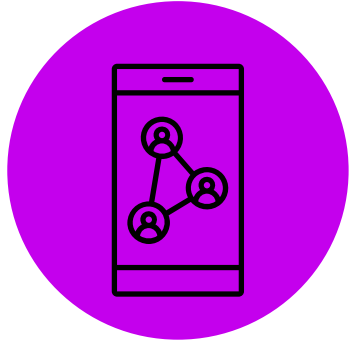
**Deceptive
promotion**



Misleading advertising and false endorsements

Where this happens matters

Different online environments create different opportunities for offenders and different forms of exposure for users.



Social media

Advertising, profiles, direct messages, sharing links and public data



Marketplaces & listings

Buying and selling with people you do not know



Messaging services

Direct, private and often personal communication



Gaming environments

In-game spending, virtual economies and opportunities for exploitation

AI: Increasing sophistication of existing fraud

Generative AI is currently described as enhancing the sophistication of existing fraud attacks, rather than creating entirely new forms of fraud.



AI-generated content, deepfakes and voice cloning can make impersonation more convincing and harder to detect.



Creating deepfakes for malicious purposes has become easier and cheaper.



The NCA warns human detection of deepfakes could become impossible by 2029.



45% of users aged 16+ who encountered deepfakes said they related to scams or fraudulent promotions.

Who is vulnerable? Children & adolescents



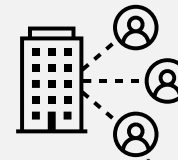
Financial exploitation of children is an emerging and under-recognised form of harm.



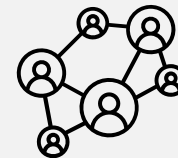
Exposed through social media, gaming and other online services: fake giveaways, phishing, fraudulent websites and more.



Risks extend to financial exploitation, including money mule recruitment.

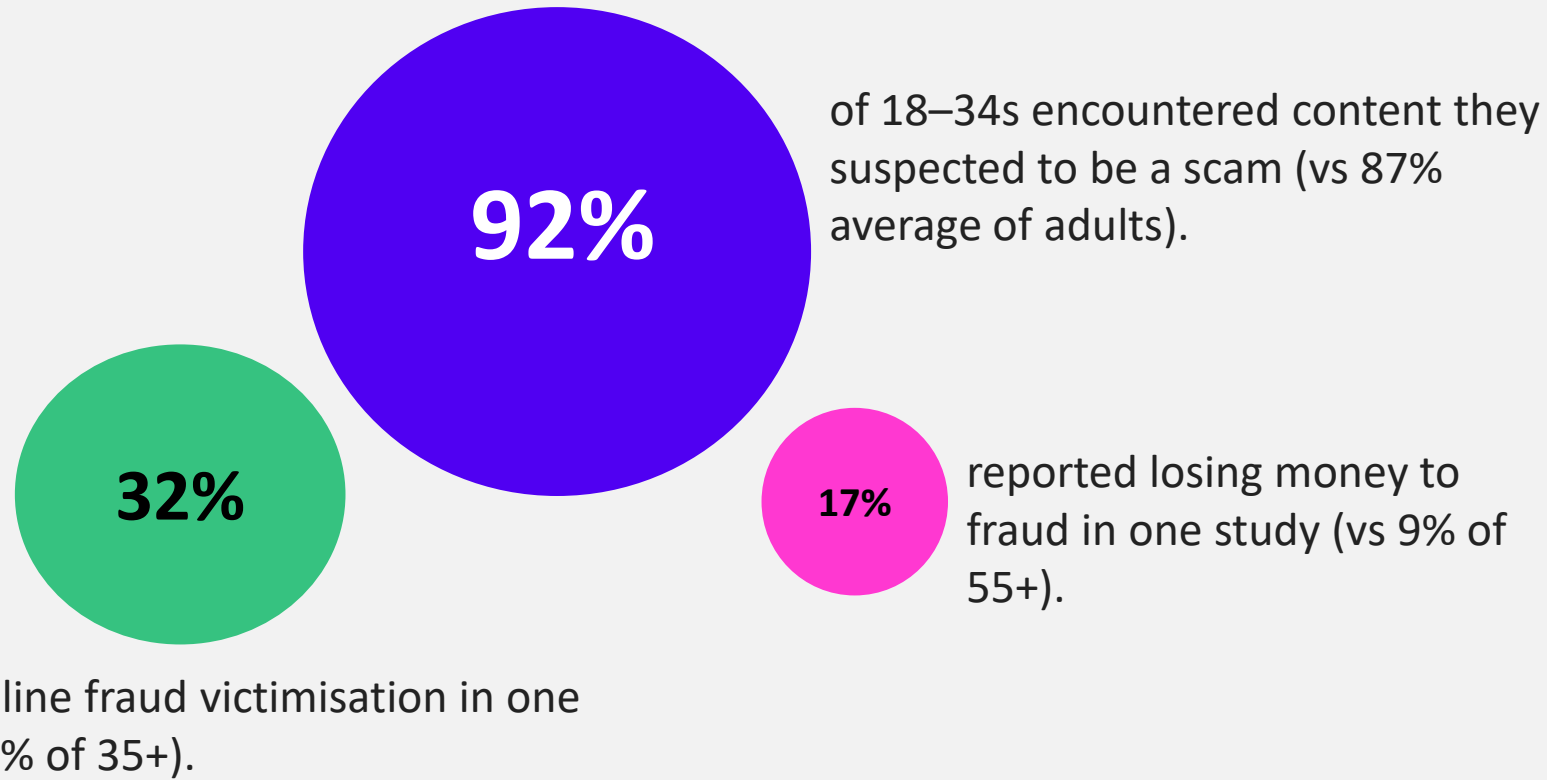


Gaps in institutional preparedness: limited awareness among professionals, institutions and regulators of emerging tactics.



Vulnerabilities include limited financial literacy, high digital engagement, developmental factors and wider socio-economic circumstances.

Who is vulnerable? Young adults (18-34)

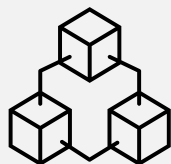


Higher digital engagement does not always mean safer behaviour: oversharing, ignoring alerts and not verifying requests.

Who is vulnerable? Older adults (65+)



Factors include lower digital literacy for some, social isolation, health-related vulnerabilities and reliance on online services.



Risks include impersonation, fake investment services, crypto offers, customer-support scams and AI-enabled deception.

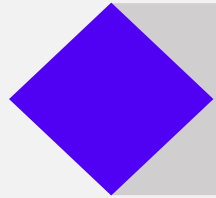


Evidence does not support assuming all older adults are more vulnerable; some studies show lower victimisation or stronger protective behaviour.

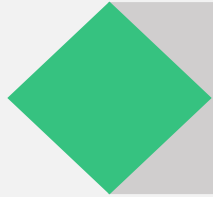


Some literature suggests repeat victimisation and higher financial losses.

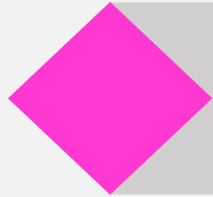
Key takeaways



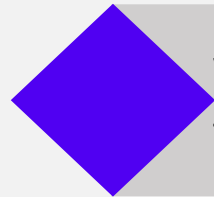
Financial manipulation is embedded across many forms of fraud.



It works through deception, trust exploitation, urgency and unrealistic rewards.



Digital environments shape exposure and opportunity.



Vulnerability varies by age and circumstance – there is no single victim profile.



AI is enhancing existing fraud by making deception more credible and harder to detect.

**Move beyond
“who is
vulnerable?” and
focus on how
vulnerability
emerges in
specific contexts.**