Financial Disinformation

Understanding Online Financial Harm: A Review of Fraud and Disinformation Exposure Across Demographic Groups in the UK

Literature Review

Published 27 November 2025

Contents

Section

Introduction

This review aims to provide an overview of literature examining how financial disinformation shared online can facilitate fraud, and understand the impact this has on victims. This literature review will inform the work of the Online Information Advisory Committee ('the Committee'), as well as others to whom it may be of interest.

The Committee has requested that the literature review cover the following topics:

a) How do different age groups in the UK access or encounter financial information online?
b) What types of online content do UK users engage with that may increase their exposure to financial harm? The emphasis is on online services where financial information is accessed or shared.
c) What are the different formats through which financial scams, and disinformation are disseminated online?
d) Who are the key actors responsible for financial scams, and disinformation in the UK?
e) How and to what extent does this content impact individuals from different demographics?

To address these topics, we have structured the literature review into three overarching sections:

a) How financial disinformation manifests in fraud online – how people search for financial information, experiences of fraud, types of fraud, content distribution, and actor types.
b) How financial disinformation through fraud impacts people of different ages.
c) Limitations, future directions and conclusions.

Methodology

Scope and definitions

Our initial research showed that the terms “scam”, “fraud”, and “disinformation” are often used interchangeably in literature examined. We therefore used all three terms in our literature search so as to ensure we captured a broad range of relevant material.

The enablers used in fraud are wide-ranging. For example, cyber-tactics which are designed to socially engineer victims into providing personal data can be used across multitudes of fraud typologies. Some of these may not use disinformation as a tactic. This review seeks to focus on forms of fraud where financial disinformation is a key tactic used in socially engineering a victim.

For the purpose of this literature review, we have looked closely at literature that involves ‘financial disinformation’ where content has been deliberately designed to deceive, manipulate, or defraud individuals, often resulting in financial harm.[1] We recognise that fraud and disinformation can have a range of impacts, however, for the purposes of this review we have focussed on instances where the immediate harm is financial, and not cases where only the secondary harm is financial.

The review has focussed on literature concerned with disinformation and the reported intent to cause financial loss/harm to individuals, and excluded literature looking at misinformation. In making this distinction for the purposes of the review, we have relied upon the definitions used by Santos-d’Amorim and Fernandes de Oliveira Miranda.[2] Their distinction hinges on intent to cause harm; however, as the literature widely acknowledges, identifying intent is often difficult. As such, this review focuses on literature explicitly reporting on instances of malicious intent or on clear evidence of financial harm to individuals.

We then considered literature which highlights how experiences of these types of fraud might impact different age groups in the UK as they access financial information online, and how this may increase their exposure to false or misleading content. This was designed to help address the Committee’s interest in how experiences might differ by age group.

Due to this interest, we have primarily used the lens of age as a factor influencing exposure to or harm from such content in this review. As a result, although other demographic factors are referenced in the review, they are not examined systematically. However, we aware of the varied harms and risks across communities.

Although email and telephone are among the most reported delivery methods for fraud,[3] [4] these forms of fraud delivery fall outside the scope of this review, as we primarily focus on online forms of communication which may be in scope of the Online Safety Act.

---

[1] Zhang, Xiaohui; Du, Qianzhou; and Zhang, Zhongju, 2022. A theory-driven machine learning system for financial disinformation detection, *Production and Operations Management*, 31:8, p. 1.
[2] Santos-d’Amorim, Karine; and Fernandes de Oliveira Miranda, Mariana, 2021. Misinformation, Disinformation, and Malinformation: clarifying the definitions and examples in disinfodemic times, *Encontros Bibli: Revista Eletrônica de Biblioteconomia e Ciência da Informação*, 26, pp. 1–23.
[3] Ofcom, 2023, Adults’ Media Use and Attitudes Report 2023, Ofcom, p. 12.
4 Re-engage, 2023, Older People’s Experiences of Scams: Findings from the Re-engage Community, Re-engage, p. 5.

Searching for relevant literature

To conduct a thorough and focused literature review, the team used a structured search strategy that began with Boolean queries and was followed by a process of refinement to tailor the results to the specific research focus.

Searches were conducted primarily through Google Scholar and general search engines. Results were filtered to include only sources published from 2020 onwards to capture the most recent developments and trends in online financial harm and disinformation. The review included grey literature from civil society organisations, safety tech firms, regulatory bodies, and industry reports in addition to peer-reviewed academic literature to capture emerging insights and practical perspectives not yet reflected in some academic publications.

The team filtered by publication date to focus on the most recent and relevant studies. To conduct a focused and relevant literature review on the ways in which fraud and disinformation cause financial harm to people in the UK, particularly across different age groups, the research team employed a structured and iterative search strategy. The initial phase involved the use of Boolean search strings to identify relevant academic and grey literature, including Ofcom publications. These queries combined key terms related to disinformation, financial harm, and demographic groups within the UK context.

Search queries were later refined to include targeted keywords to drill down into specific forms of financial disinformation and demographic impacts.

Sources were selected based on their relevance to the research questions, credibility, and contribution to understanding the intersection of digital disinformation and financial harm across age groups.

How financial disinformation manifests through fraud online

Overview of the scale of fraud in the UK

Fraud remains one of the most significant threats to individuals and the UK economy. The National Security Strategy (2025) highlights the estimated total cost of fraud to society against individuals is a minimum of £6.8 billion.[5] As financial activity increasingly shifts online, people are more frequently exposed to fraudulent practices and misleading financial content.

The latest findings from the Crime Survey for England and Wales (year ending March 2025) highlight the continued rise in fraud. Compared with 2024, incidents increased by 31%, reaching an estimated 4.2 million cases. Fraud now makes up 41% of all crime captured in the survey and was a key driver of the 7% overall rise in headline crime.[6]

Fraud levels remain significantly above the pre-pandemic baseline, reflecting the long-term shift towards "living online" that accelerated during the pandemic.[7] An estimated 60% of fraud incidents are cyber-related, with high-harm categories such as investment fraud and romance fraud persisting at pandemic-era levels.

According to the Office for National Statistics, the increase in 2025 was driven primarily by:

- Banking and payment fraud – including fraudulent use of bank cards and online banking.
- Consumer and retail fraud – involving online shopping, counterfeit goods, and non-delivery scams.
- Advance fee fraud – where victims pay for goods or services that are never delivered.
- Other fraud – including investment, romance, and identity fraud.[8]

Despite the scale of harm, reporting remains low. Only around 14% of frauds against individuals are reported to Action Fraud.[9] Trends in reporting continue to show investment and romance fraud at high levels, consistent with patterns first observed during the pandemic.[10]

Fraud affecting UK victims frequently has an international dimension. The cyber-enabled nature of these crimes and the laundering of criminal proceeds often span multiple jurisdictions. In most cases, victims do not know who has targeted them: in the year ending March 2023, only 9% of adult victims were able to provide any information about offenders.[11]

---

[5] HM Government, 2025. National Security Strategy 2025 Security for the British people in a dangerous world.
[6] Office for National Statistics, 2025. Crime in England and Wales: year ending March 2025, Statistical Bulletin, released 24 July 2025.
[7] Office for National Statistics 2025. Crime in England and Wales: year ending March 2025, Statistical Bulletin, released 24 July 2025.
[8] Office for National Statistics 2025. Crime in England and Wales: year ending March 2025, Statistical Bulletin, released 24 July 2025.
[9] National Crime Agency, 2025. National Strategic Assessment 2025: Fraud, National Strategic Assessment of Serious and Organised Crime.
[10] National Crime Agency, 2025. National Strategic Assessment 2025: Fraud, National Strategic Assessment of Serious and Organised Crime.
[11] National Crime Agency, 2025. National Strategic Assessment 2025: Fraud, National Strategic Assessment of Serious and Organised Crime.

Overall, an estimated 67% of fraud reported in the UK is cyber-enabled. Authorised push payment frauds are increasingly linked to the abuse of online platforms. Social media, in particular, is a key enabler of fraud, providing channels for contact through adverts and direct messages. It is a major facilitator of online shopping scams, ticket fraud, and investment fraud. A growing concern has been the rise of social media account hacking, which has been used to promote fraudulent ticket sales and has contributed to the continued increase in ticket fraud cases.[12]

Reported experiences of fraud in the UK

Recent data from Ofcom (2023) reveal the scale of public exposure to potentially harmful online content: nearly nine in ten UK adult internet users (87%) report encountering material they believe to be fraudulent or part of a scam. Almost half (46%) say they have engaged with an online scam or fraud attempt, and 39% report knowing someone who has fallen victim to an online scam or fraud attempt.

Although banks and financial advisors remain primary sources of financial information[13], there is a noticeable shift toward digital alternatives. For example, a recent study by Capital One (2024) found that 13.7% of UK adults now rely on social media for financial information.[14] This suggested that there is high-risk for individuals using online sources for financial information as most content on one service examined was assessed to be generated by entities who had no recognised qualifications or regulatory oversight.[15] This analysis stated that individuals who engage with these sources tend to perform worse on financial literacy assessments, suggesting a strong correlation between exposure to unregulated content and susceptibility to financial harm.[16]

A review by the Parliamentary Office of Science and Technology observed that research consistently highlights the impacts of fraud on victims.[17] Financial harm often has other harms related to it, extending beyond financial loss, encompassing emotional, psychological, and practical consequences for both individuals and businesses. Even when the sums involved are relatively modest, victims often report significant distress, fear of being targeted again, and a diminished sense of trust in online or financial systems.[18] These harms are often harder to measure because they do not always correspond directly to the monetary value lost.[19] Victims often experience a range of emotional and psychological harms, including shame, anxiety, anger, trauma, and diminished self-confidence.[20] These effects can also manifest in poorer mental and physical health outcomes. In many cases, the aftermath of fraud can disrupt personal relationships, contributing to social isolation and loneliness. Moreover, victims may adopt long-term behavioural changes – such as increased mistrust or

[12] National Crime Agency, 2025. National Strategic Assessment 2025: Fraud, National Strategic Assessment of Serious and Organised Crime.
[13] Capital One, 2024. Where do people go for financial guidance?
[14] Capital One, 2024. Where do people go for financial guidance?
[15] Capital One, 2024. Where do people go for financial guidance?
[16] Capital One, 2024. Where do people go for financial guidance?
[17] Natalie Low and Clare Lally, 2024. Social and psychological implications of fraud, POST note 720, UK Parliament, p. 9.
[18] Levi, M, 2023. Written evidence submitted by Professor Michael Levi – The impacts of frauds and responses to them.
[19] Levi, M, 2023. Written evidence submitted by Professor Michael Levi – The impacts of frauds and responses to them.
[20] Natalie Low and Clare Lally, 2024. Social and psychological implications of fraud, POST note 720, UK Parliament, p. 11.

withdrawal from online or financial activity.[21] This means that harms stemming from fraud include financial loss, and often also less-visible but significant emotional and psychological harms.

Globally low financial literacy levels further exacerbate these risks. Research from the Organisation for Economic Co-operation and Development (OECD) highlights persistently low levels of financial literacy among populations worldwide. According to the OECD, this creates fertile ground for fraudsters to exploit gaps in both financial and digital knowledge. Fraudsters increasingly capitalise on this dual vulnerability, using deceptive tactics to manipulate consumer behaviour and encourage harmful financial decisions.[22]

Formats of financial disinformation

The literature examined in this review highlighted that some forms of fraud involve financial disinformation as a means of social engineering.[23]

According to the National Crime Agency (2025), online offenders are increasingly taking advantage of greater connectivity to offend on a larger scale. Fraud criminals use online platforms to deceive users, for example offering goods or services that do not exist, or a platform's algorithm to deliver targeted advertisements to potential victims.[24]

The literature also highlights fraud criminals will exploit a user's trust of what they encounter online by falsely imitating legitimate services or trusted institutions.

Several of the sources analysed in this literature review noted that, regardless of the specific format, most frauds share core psychological tactics: they create a false sense of urgency and promise unrealistic rewards, pressuring individuals to act without verifying the legitimacy of the offer. Deception was identified as a factor leading to the fraud being carried out, as it impacts trust and decision-making, and therefore represent financial disinformation in practice.

The Financial Conduct Authority (FCA) has published advice on fraud which claims financial legitimacy by pretending to be from an FCA-authorised or regulated service. Common tactics include **phishing emails**, **fraudulent phone calls, counterfeit websites**, and the **impersonation of official bodies.**[25] Social media, private messaging services and online marketplaces are increasingly leveraged by fraud criminals to deceive individuals into disclosing sensitive information or transferring funds. Certain types of fraud rely on upfront payments, such as **loan fee fraud.** The FCA reported that fraudsters often ask for between £25 and £450 as a fee for a loan, sometimes falsely claiming it is refundable. The fraudster may claim the fee is an administrative or insurance for the loan, or required because the victim has bad credit history.[26] Others employ technical methods to compromise security, including the use of screen-sharing tools or **ransomware** to gain unauthorised

[21] Natalie Low and Clare Lally, 2024. Social and psychological implications of fraud, POST note 720, UK Parliament, p. 11.
[22] OECD, 2016. OECD/INFE International Survey of Adult Financial Literacy Competencies; OECD, 2017. G20/OECD INFE Report on Adult Financial Literacy in G20 Countries. OECD; both as cited in: Lapuh Bele, J. (no date). Financial Scams, Frauds, and Threats in the Digital Age, p. 39.
[23] 'Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.' Home Office Digital, Data and Technology, no date. Cyber Security.
[24] National Crime Agency, 2025. National Strategic Assessment 2025: Cross-Cutting Threat Enablers, National Strategic Assessment of Serious and Organised Crime.
[25] Financial Conduct Authority, 2025. Protect yourself from scams, Financial Conduct Authority, first published 8 August 2017, last updated 21 May 2025.
[26] Financial Conduct Authority, 2025. Loan fee fraud.

access to personal accounts.[27] The FCA states that those behind this activity can try to build a false sense of trust or security to encourage a victim to give them control of their screen to access personal information.[28]

Citizens Advice highlighted that investment-related frauds typically involve high-risk financial schemes that are falsely presented as lucrative opportunities.[29] It stated that these involved convincing a person to move their money for a fake investment which does not exist.

Research commissioned by Ofcom found that **impersonation fraud** was the most experienced type of online fraud, reported as being experienced by 51% of respondents.[30] UK Finance has said that impersonation fraud involves criminals falsely pretending to be trusted organisations or individuals to persuade victims to share personal or financial information or make payments.[31] This false identity might be combined with 'true' information gathered from other scams and data breaches to make their approach sound genuine.

Other commonly-reported forms of fraud also rely on misrepresentation or false promises. These include counterfeit goods scams (42%), investment or "get rich quick" schemes (40%), and computer software or ransomware scams (37%). Further categories, such as fake employment scams, and health scams, all exploit trust by presenting fabricated beneficial opportunities or identities to cause financial harm.[32]

False or deceptive debt advice has been flagged by the Advertising Standards Authority (ASA) as a growing concern in online financial information sharing. A 2021 ruling found that commercial firms were using paid search ads to **impersonate legitimate debt charities** and exaggerate the ease of debt resolution, misleading vulnerable users into unsuitable financial solutions.[33]

The use of generative artificial intelligence (GenAI) as an enabler of serious and organised crime is expected to grow in 2025, particularly in relation to fraud, cybercrime, and child sexual abuse.[34] The deliberate creation of deepfakes for malicious purposes has also become easier and cheaper.[35] The National Crime Agency warns that human detection of deepfakes will become impossible by 2029, with some industry figures predicting that by 2025 even the best specialists will be unable to distinguish them from genuine media.[36] The National Strategic Assessment's current assessment of the GenAI threat in fraud indicates it is used to enhance the sophistication of fraud attacks against individuals and businesses, rather than create entirely new ones. It uses CEO fraud as an example of how it is utilised, and the increasing challenge this will present for detection. In this case study, GenAI was used to create deepfakes of company employees at a virtual meeting and convinced a

[27] Financial Conduct Authority, 2025. Protect yourself from scams, first published 8 August 2017, last updated 21 May 2025.
[28] Financial Conduct Authority, 2025, Screen sharing scams.
[29] Citizens Advice, 2024. 9 million people caught out by financial scams in the past year.
[30] Ofcom, 2023. Online Scams & Fraud Research: Executive Summary, prepared by Yonder Consulting, p. 5.
[31] UK Finance, 2025, Annual Fraud Report 2025, UK Finance, p. 16.
[32] Ofcom, 2023. Online Scams & Fraud Research: Executive Summary, prepared by Yonder Consulting, p. 5.
[33] Advertising Standards Authority, 2021. ASA takes action against misleading debt advice ads.
[34] National Crime Agency, 2025. National Strategic Assessment 2025: Cross-Cutting Threat Enablers, National Strategic Assessment of Serious and Organised Crime.
[35] National Crime Agency, 2025. National Strategic Assessment 2025: Cross-Cutting Threat Enablers, National Strategic Assessment of Serious and Organised Crime.
[36] National Crime Agency, 2025. National Strategic Assessment 2025: Cross-Cutting Threat Enablers, National Strategic Assessment of Serious and Organised Crime.

finance worker that a requested transfer of £20 million into a criminally-controlled account was genuine and authorised by senior management.[37]

Common service types used for dissemination and distribution

Both fraud exposure and the nature of fraud are strongly shaped by the design and dynamics of a wide range of specific online services. The service design and user behaviour can increase the risk of exposure to financial disinformation and other tactics to engage individuals, increasing the risk of victimisation. The literature reviewed indicates that the service types that different groups engage with vary based on age and other characteristics. Social media, messaging and gaming services, and online marketplaces are repeatedly identified as high-risk environments due to their peer-to-peer nature, limited moderation, and the ease with which deceptive content can be disseminated.

Social media services are now one of the most common services through which frauds occur according to the literature examined. Several major UK banks report that between 60% and 77% of all frauds now originate on social media and other services.[38] TSB reported that impersonation scams on a messaging service had tripled, while Lloyds noted that fake listings on an online marketplace had doubled in the past year.[39] These services often host fraudulent advertising that use synthetic or AI-generated content. According to Ofcom's Online Scams & Fraud Research, 23% of users encountered fraud via social media, and 18% through specific websites or apps.[40]

Numerous sources cited AI-generated content, including deepfakes, as increasingly being used to enhance the credibility of scams.[41] [42] [43] Deepfake technology is a rising concern, particularly in the context of fraudulent advertising. In Ofcom's Online Nation 2024 research, 45% of users aged 16+ who said they had encountered deepfake content said it related to scams or fraudulent promotions. Those aged 55+ reported being slightly less likely to see deepfakes, but of the deepfakes they saw a higher proportion were scam-related deepfakes compared to other age groups, with 54% having encountered them, compared to 33% of users aged 16–24.[44]

Popular marketplace and listing services are repeatedly cited as hotspots for fraud. A report by Parent Zone described an attempt to defraud one user through a fake PayPal confirmation email after they listed an item for sale.[45] Lloyds also reported that fraudulent product listings had doubled year-on-year, reflecting a broader trend of scams exploiting user-to-user commerce.[46]

Ofcom's findings show that the tactics used by fraudsters differ by service type. Impersonation (51%) and ransomware (41%) were most frequently experienced via email, while romance and counterfeit good frauds were more common on websites and apps.[47]

---

[37] National Crime Agency, 2025. National Strategic Assessment 2025: Fraud, National Strategic Assessment of Serious and Organised Crime.
[38] Nominet, 2023. Digital Youth Index 2023, p. 33.
[39] Nominet, 2023. Digital Youth Index 2023, p. 33.
[40] Ofcom, 2023. Online Scams & Fraud Research: Executive Summary, prepared by Yonder Consulting, p. 12.
[41] Ofcom, 2023, Adults' Media Use and Attitudes Report 2023, Ofcom, p. 12.
[42] Nominet, 2023. Digital Youth Index 2023,, p. 33.
[43] Ofcom, 2024. Online Nation 2024, Ofcom, p. 95.
[44] Ofcom, 2024. Online Nation 2024, Ofcom, p. 95.
[45] Parent Zone, 2025. Short changed and out of time: A report into families facing financial harms alone, p. 12.
[46] Nominet, 2023. Digital Youth Index 2023, p.33.
[47] Ofcom, 2023. Online Scams & Fraud Research: Executive Summary, prepared by Yonder Consulting, p. 12.

The literature seems to suggest, therefore, that a user's exposure to potentially harmful fraud content and the form it takes is strongly influenced by the features and dynamics of specific service types. Services with high volumes of peer-to-peer interaction, such as social media, messaging apps, and marketplaces, are often reported to be more fertile ground for fraudsters. Meanwhile, the emergence of AI-generated content adds another layer of complexity and risk for consumers navigating digital spaces.

We have also considered Ofcom's chapter on fraud in the Illegal Harms Register of Risk which highlights social media services, messaging services, and marketplaces and listings services as types of services which a range of evidence analysed by Ofcom suggests are used for fraud.[48] Ofcom's Illegal Harms Register of Risk also identifies additional functionalities that can be attractive to fraudsters, including the ability to create fake user profiles; the functionality of posting goods or services for sale; being able to search user-generated content; hyperlinking and the identification of potential victims through information on user profiles and the ability to comment on content.[49]

Common actor types

There are no distinct groups or common actors in online financial fraud. The United Nations Office on Drugs and Crime's issue paper on organised fraud highlighted that[50]:

- Fraudsters can range from highly motivated groups to opportunistic individuals.
- Even within organised groups, the structure can be diverse, ranging from groups with a rigid hierarchy, a core group with a horizontal structure around it and used as required; to networks of individuals with shifting alliances who come together for specific roles or for the life cycle of a fraud.
- Some organised groups only exist online or are a mix of offline and online networks.

This diversification could be attributed to the nature of fraud offending, which is primarily concerned with financial gain using deceitful tactics that are difficult to distinguish between legitimate/ illegitimate entities, can be conducted remotely targeting victims globally and enabled by technology that enables anonymous communication and rapid transfer of the proceeds of fraud, operating across international borders.

The complexity of fraud requires a network of co-offenders, with varying degrees of awareness and complicity in the fraud – this can include cybercriminals for access/data harvesting, professional enablers such as affiliate marketers to obtain leads and telephone operators to turn a lead into a victim.

However, we have identified some common themes and patterns in the literature, and have therefore presented our review in relation to three broad categories of actors associated with online financial fraud. These are: (1) direct individual actors, such as deceptive financial influencers, impersonators, money mule recruiters, or independent fraudsters acting knowingly and with intent; (2) direct group actors, including organised fraud networks and coordinated influencer networks operating collectively; and (3) indirect/intermediate actors, such as affiliate marketers, exploitative intermediaries, or those who contribute to the spread of fraudulent content through mechanisms such as fake endorsements or clickbait, and may or may not be fully aware of their role in fraud ecosystems. Although this typology does not always mirror the way most literature is structured, it

[48] Ofcom, 2024. Register of Risks, p. 235.
[49] Ofcom, 2024. Register of Risks, pp. 234-245.
[50] United Nations Office on Drugs and Crime (UNODC), 2024. Organized Fraud: Issue Paper, pp. 15-19.

provides a structural and practical basis for reviewing the evidence and analysis presented in the literature.

'Direct individual actors'

A significant proportion of online financial fraud is initiated or executed by individuals acting independently. Among the most documented categories are some financial influencers ("finfluencers") using deceptive means to engage in fraud,[51] and money mule recruiters, both of whom can knowingly engage in fraudulent or high-risk activity directed at consumers.[52]

In the UK, the FCA suggests that finfluencers, often operating on popular social media services, may promote unauthorised, high-risk, or non-existent financial products while portraying themselves as credible financial experts. The FCA has taken enforcement action against individuals in this category, including formal interviews under caution for breaches of financial promotion rules.[53]

On the other hand, money mule recruiters often target financially vulnerable people through fake job adverts, convincing them to move illicit funds via their personal accounts. The UK saw a surge in this tactic during the COVID-19 pandemic.[54] The Government's own action plan recognises the systematic nature of this grooming and notes that many recruits are unaware of the criminal implications.[55]

Finfluencers and mule recruiters form part of a broader group of individuals who act knowingly to perpetrate fraudulent schemes. This includes those involved in impersonation fraud, unauthorised investment offers and other financial deception schemes.[56]

'Organised group actors'

Fraud is also frequently orchestrated by structured groups. These operations often involve coordinated activities executed at scale. Royal United Services Institute (RUSI) has referred to organised fraud as an "emerging epidemic" in the UK, pointing to the involvement of multi-role criminal networks that use both digital infrastructure and human actors to defraud victims.[57]

Research carried out by the UN has demonstrated that organised criminal groups use a wide range of fraud formats that often mirror legitimate commercial or financial activity, making them difficult for consumers to identify and regulators to disrupt.[58] The UN report shows that types of fraud are typically structured around persuasive narratives—such as offering high-yield investments, employment opportunities, or urgent debt repayment demands—and are executed at scale through digital services.[59] Common formats include the sale of non-existent or misrepresented consumer goods and services, often marketed through fake websites, hijacked seller profiles, or social media advertisements. Employment fraud schemes offer fictitious jobs or business opportunities, frequently requiring upfront payments for training, equipment or checks, and sometimes draw

---

[51] FCA, 2025. FCA leads international crackdown on illegal finfluencers.
[52] UK Finance, 2020. Half Year Fraud Update 2020.
[53] FCA, 2025. FCA leads international crackdown on illegal finfluencers.
[54] UK Finance, 2020. Half Year Fraud Update 2020.
[55] Home Office, 2024. Money mule and financial exploitation action plan, p. 10.
[56] Skidmore, Michael; Aitkenhead, Beth, 2023. Understanding the Characteristics of Serious Fraud Offending in the UK, Police Foundation, pp. 2, 9, 12.
[57] Wood, H., Keatinge, T., Ditcham, K. and Janjeva, A., 2021. The Silent Threat: The Impact of Fraud on UK National Security, Royal United Services Institute for Defence and Security, p. vii.
[58] United Nations Office on Drugs and Crime (UNODC), 2024. Organized Fraud: Issue Paper, pp. 21–27.
[59] United Nations Office on Drugs and Crime (UNODC), 2024. Organized Fraud: Issue Paper, pp. 21–27.

victims into further criminality such as money mule activity.[60] Money mule networks also form a part of this category.[61] Consumer investment fraud, including fraudulent cryptocurrency services and Ponzi-style schemes, often promise exaggerated returns and may involve cloned websites or impersonated financial professionals. These fraudulent schemes have become increasingly sophisticated, with offenders adopting the language, branding and structure of regulated firms to cultivate legitimacy.[62] A notable example of this type of fraud is the OneCoin fraud scheme. OneCoin, launched in 2014 and headquartered in Sofia, Bulgaria, was promoted as a legitimate cryptocurrency but in reality, operated as a fraudulent scheme distributed through a global multi-level-marketing network. Through widespread misrepresentations the scheme drew in millions of victims worldwide and generated more than $4 billion in investments.[63]

Regulatory gaps and cross-border coordination challenges make these operations harder to detect and disrupt, while victims often lose substantial sums before realising they have been defrauded.[64] The UN Office on Drugs and Crime notes that organised fraud schemes continuously evolve to exploit emerging technologies, regulatory blind spots, and shifts in consumer behaviour, with some groups operating through supply-chain-style models involving multiple layers of perpetrators.[65]

The 2025 National Strategic Assessment highlighted some changes in risk and impact from serious and organised crime (SOC) related to fraud in the UK:[66]

- The SOC threat in the UK grew in 2024 but at a slower pace than in the previous, post-pandemic period. It is likely that the fraud threat to UK individuals and businesses has increased since 2023, although estimated fraud levels are similar to those last seen in 2019.
- This growth in SOC is principally being driven by online connectivity and the growth of automation technology.
- Online connectivity underpins a wide variety of offending including child sexual abuse, cybercrime, and fraud, and enables almost all serious and organised criminality in some form. SOC offenders are increasingly exploiting advances in technology to access victims and cause them harm on a larger scale, connect with global networks, and enhance their adaptability and resilience to disruption.
- The population's routine dependence on online services continues to provide opportunities for fraud offenders to target victims, sustaining the UK's vulnerability to fraud. Industry prevention measures continue to contain the threat from fraud to some extent, but some fraud types, such as card-not-present fraud, are increasing.

'Indirect or intermediary actors'

Indirect actors play a facilitative role, often contributing to fraud through marketing, advertising, or hosting infrastructure. A key group within this category includes affiliate marketers—individuals or companies paid to generate leads or web traffic for fraudulent schemes. Investigations have shown that organised fraud operations outsource this function to third-party agencies that specialise in placing misleading or sensationalist ads. The marketers are often paid if a lead goes on to engage

[60] United Nations Office on Drugs and Crime (UNODC), 2024. Organized Fraud: Issue Paper, pp. 21–27.
[61] HM Government, 2023. Fraud Strategy: Stopping Scams and Protecting the Public, updated 1 June 2023.
[62] United Nations Office on Drugs and Crime (UNODC), 2024. Organized Fraud: Issue Paper, pp. 21–27.
[63] United States Attorney's Office, Southern District of New York, 2023. Co-Founder Of Multibillion-Dollar Cryptocurrency Scheme "OneCoin" Sentenced To 20 Years In Prison.
[64] United Nations Office on Drugs and Crime (UNODC), 2024. Organized Fraud: Issue Paper, pp. 14–73.
[65] United Nations Office on Drugs and Crime (UNODC), 2024. Organized Fraud: Issue Paper, pp. 21-27.
[66] National Crime Agency, 2025. National Strategic Assessment, 2025.

with the fraud. This indicates either complicity in facilitating the fraud or unethical practices by not checking the legitimacy of the product or service they promote.[67]

One frequently used tactic in such advertising involves fabricated celebrity endorsements. According to the UK's National Cyber Security Centre (NCSC), a significant proportion of fraud content in 2021 promoted fake investment offers using doctored images or false statements attributed to well-known public figures. As part of the Active Cyber Defence programme, more than 600,000 URLs linked to these scams were taken down. Despite their varied appearance, these tactics consistently sought to exploit trust in high-profile individuals to encourage users to interact with fraudulent financial material.[68]

[67] McLennan, Malina; Coluccini, Riccardo; 2025, Scam Operations Relied on Third-Party Marketing Companies for Steady Stream of Potential Victims, OCCRP, 7 March 2025.
[68] National Cyber Security Centre (NCSC), 2022. Active Cyber Defence: The 5th Year – Summary of Key Findings, p. 8.

Demographic segmentation of victims of online fraud

A study by Dadà et al emphasises that fraud victims represent a diverse population and should not be treated as a single, homogenous group.[69] Victimisation typically results from a combination of factors, including the fraud format, personal traits of the victim, and situational contexts. Most instances of fraud take place online.[70] Vulnerability to fraud affects all age groups, though certain fraud formats are more common in specific demographics.[71] Across various studies, the most consistently linked risk factors include lower levels of conscientiousness, higher impulsivity, cognitive decline, and social isolation.[72]

Evidence from the Crime Survey for England and Wales (CSEW) also indicates that while fraud affects a broad cross-section of the population, certain socio-demographic groups face slightly elevated risks. In the year ending March 2023, 6.3% of adults were estimated to have experienced fraud.[73] However, higher rates were observed among women aged 25–44, individuals in higher income or education brackets, those in managerial roles, as well as among groups considered potentially vulnerable, such as single parents and LGBT individuals.[74] Although the variation in fraud risk is less pronounced than for other types of crime, these patterns suggest that exposure is not evenly distributed.[75] Some commentators, such as Low and Lally, have noted that prevailing stereotypes—such as the notion that elderly people are the most common victims—are both misleading and unsupported by current data.[76] Research by Ofcom showed that older age groups (65+) were better able to identify a form of fraud.[77] Ofcom showed respondents a screenshot of a fake email purporting to be from a parcel delivery company and asked them how they would respond. Over eight in ten (83%) online adults responded appropriately to the email, by saying they would take an action such as deleting it, reporting it or blocking the sender. Other actions, such as replying or clicking on links in the email, may risk someone accidentally downloading malware or start the

[69] Dadà, Chiara Barbara; Colautti, Laura; Rosi, Alessia; Cavallini, Elena; Antonietti, Alessandro; and Iannello, Paola, 2025. Uncovering vulnerability to fraud and scams among adult victims in online and offline contexts: A systematic review, Computers in Human Behavior.
[70] Dadà, Chiara Barbara; Colautti, Laura; Rosi, Alessia; Cavallini, Elena; Antonietti, Alessandro; and Iannello, Paola, 2025. Uncovering vulnerability to fraud and scams among adult victims in online and offline contexts: A systematic review, Computers in Human Behavior.
[71] Dadà, Chiara Barbara; Colautti, Laura; Rosi, Alessia; Cavallini, Elena; Antonietti, Alessandro; and Iannello, Paola, 2025. Uncovering vulnerability to fraud and scams among adult victims in online and offline contexts: A systematic review, Computers in Human Behavior.
[72] Dadà, Chiara Barbara; Colautti, Laura; Rosi, Alessia; Cavallini, Elena; Antonietti, Alessandro; and Iannello, Paola, 2025. Uncovering vulnerability to fraud and scams among adult victims in online and offline contexts: A systematic review, Computers in Human Behavior.
[73] Low, Natalie; Lally, Clare; 2024, Social and psychological implications of fraud, POSTnote 720, UK Parliament POST, published 29 April 2024, https://researchbriefings.files.parliament.uk/documents/POST-PN-0720/POST-PN-0720.pdf pg. 8.
[74] Low, Natalie; Lally, Clare; 2024, Social and psychological implications of fraud, POSTnote 720, UK Parliament POST, published 29 April 2024, p. 8.
[75] Low, Natalie; Lally, Clare; 2024, Social and psychological implications of fraud, POSTnote 720, UK Parliament POST, published 29 April 2024, p. 8.
[76] Low, Natalie; Lally, Clare; 2024, Social and psychological implications of fraud, POSTnote 720, UK Parliament POST, published 29 April 2024, p. 8.
[77] Ofcom, 2025. Adults' Media Use and Attitudes Report, p. 18.

process for a scammer to demand money. This was a decrease from the 86% of online adults who responded appropriately last year, and from 88% in 2022. Similarly to the paid partnerships and search engine advertising tests, it was the older age groups who were more likely to respond correctly, such as those aged 65+ (92%); in comparison, only 70% of 25-34s took the appropriate action.

Age is not consistently categorised across the literature, making it difficult to apply uniform age bands when reviewing evidence. However, adopting a working age framework was necessary to structure and make sense of the findings.

Children Under 13, Adolescents and Teens (13–17)

Due to limitations in the literature examined, which often combine children under 13 and adolescents into a single category, this section groups the two age ranges together to better reflect the available evidence.

Evidence shows that children face risks of financial harm in online environments.[78] Children between the ages of 8 and 17 are increasingly exposed to online financial scams, with 9% reporting personal financial loss, including children as young as eight.[79] A further 18% said they knew someone their age who had lost money to an online scam.[80] The most common scam types included fake giveaways, phishing scams, fake websites, online shopping scams, and trust trades in online games.[81] Social media was identified as the most frequent service type through which scams were encountered (35% overall, including 30% of children aged 12 and under), followed by email (17%) and online games (15%), with 22% of children aged 8–11 encountering scams in gaming environments.[82]

Financial exploitation of children is an emerging and under-recognised form of abuse. The Children's Society (2025) conducted interviews with 17 specialist professionals working directly with children affected by exploitation. These included frontline practitioners and managers with experience supporting children under 18 and their families. The study identifies child financial exploitation, including exploitative money laundering, as a growing and under-recognised form of abuse affecting children under 18.[83] Children may be manipulated or coerced into moving money through bank or streaming accounts, making purchases from illegitimate businesses, or returning stolen goods for refunds. Exploiters also target children's financial resources directly, including prepaid spending cards and welfare benefits, sometimes through familial or intimate relationships where control over the child's finances is exerted.

Recruitment often occurs via social media and messaging services, where exploiters use fake profiles and job adverts to lure children into schemes that appear legitimate. Online gaming environments including gaming services are also used to build trust and normalise financial transactions through virtual rewards. Children are particularly vulnerable due to limited financial literacy, high digital engagement and susceptibility to manipulation. Socioeconomic factors such as poverty, parental neglect, exposure to household violence and exclusion from mainstream

[78] Nominet, 2023. Digital Youth Index 2023, p.33.
[79] UK Safer Internet Centre; 2024, *Almost half of 8 to 17 year olds have been scammed online*, published 6 February 2024, available at: https://saferinternet.org.uk/blog/almost-half-of-8-to-17-year-olds-have-been-scammed-online.
[80] UK Safer Internet Centre, 2025. Almost half of 8 to 17 year olds have been scammed online.
[81] UK Safer Internet Centre, 2025. Almost half of 8 to 17 year olds have been scammed online.
[82] UK Safer Internet Centre, 2025. Almost half of 8 to 17 year olds have been scammed online.
[83] The Children's Society, 2025. Moving Money, pp. 3–30.

education further increases risk. Despite these vulnerabilities, the study highlights a lack of awareness among safeguarding professionals and financial institutions, with inconsistent responses and limited support structures contributing to missed opportunities for early intervention.[84] This research by the Children's Society points to a lack of preparedness among safeguarding professionals, financial institutions, and regulators in recognising and responding to emerging forms of financial exploitation, particularly those affecting children and adults (aged 18 to 34).[85] The Children's Society, Ofcom, the FCA, and the Home Office have all pointed to the limited awareness of tactics such as money mule recruitment, financial grooming, and the use of synthetic or AI-generated content media in fraudulent campaigns.[86] [87] [88] [89]

In addition to findings from professionals and researchers, parents also report a wide range of money-related harms affecting their children online. According to Parent Zone (2025), 20% of UK parents reported that their child had encountered a money-related problem online. These incidents range from accidental purchases and unmanageable subscriptions to more serious forms of harm such as identity theft, unauthorised withdrawals, and financial grooming. Notably, 9% of children were offered money to hold funds for others (indicative of money mule schemes), and 8% were offered money in exchange for naked images—equivalent to an estimated 846,000 and 752,000 children respectively.[90] Among digitally active children, 42% reported accidentally subscribing to services, being scammed, or losing money online in some other way.[91]

Despite growing evidence of harm, financial risks to children online remain under-recognised, with girls more likely than boys to report experiences of scams and fraud. Two studies suggest that financial risks to children online are frequently under-recognised.[92] [93] This is often attributed to assumptions that children are not active financial agents or that the sums involved are too minor to warrant serious concern.[94] However, emerging evidence challenges these views. Parent Zone (2023) reports that 68% of 13–18-year-olds have some form of financial agency online—whether through spending, earning, or storing money, either independently or with assistance. Moreover, 14% of children under 18 believe they have been scammed, including through non-delivery of paid goods or theft of in-game points.[95] According to the 2023 Digital Youth Index, 14% of 12–18-year-olds reported being targeted by an online scam in the previous year—up from 10% in 2022. In total, 35% of 12–18-year-olds had encountered some form of scam, rising to 50% among those aged 16 and above.[96] Ofcom (2024) similarly found that 24% of boys and 23% of girls aged 13–17 reported that

[84] The Children's Society, 2025. Moving Money, pp. 3–30.
[85] The Children's Society, 2025. Moving Money, pp. 3–30.
[86] The Children's Society, 2025. Moving Money, pp. 3–30.
[87] Ofcom, 2023. Online Scams & Fraud Research: Executive Summary, prepared by Yonder Consulting, p. 12.
[88] Financial Conduct Authority, 2025. Protect yourself from scams, first published 8 August 2017, last updated 21 May 2025.
[89] Home Office, 2024. Money mule and financial exploitation action plan, p. 10.
[90] Parent Zone, 2025. Short changed and out of time: A report into families facing financial harms alone, p. 12.
[91] Parent Zone, 2023. A Problem Hiding in Plain Sight? Children Spending, Making and Losing Money Online, p. 7.
[92] Nominet, 2023. Digital Youth Index 2023, p. 33.
[93] Parent Zone, 2023. A Problem Hiding in Plain Sight? Children Spending, Making and Losing Money Online, p. 5.
[94] Parent Zone, 2023. A Problem Hiding in Plain Sight? Children Spending, Making and Losing Money Online, p. 5.
[95] Parent Zone, 2023. A Problem Hiding in Plain Sight? Children Spending, Making and Losing Money Online, p. 15.
[96] Nominet, 2023. Digital Youth Index 2023, p. 33.

they had experienced scams, fraud, or phishing attempts online.[97] Risk exposure is not evenly distributed: girls were more likely than boys to report scam experiences (39% vs. 31%), and rates were also higher among LGBTQ+ youth (50%) and people aged 11-25 with disabilities (40%).[98]

Rising financial losses among under 13 and adolescents are also observed in datasets beyond the UK. Data from the US supports the view that teens are among the fastest-growing cohorts of online scam victims. According to Social Catfish (2023), financial losses among those aged 20 and under in the US rose from $8.2 million in 2017 to $210 million in 2022, a nearly 2,500% increase. While US-based, this trend is consistent with UK concerns: Action Fraud reported over 1,000 UK children and teenagers were scammed each month in 2022.[99]

Findings also highlight the emergence of more sophisticated fraud techniques. Child users aged 16-18 and adult users aged 18-24 are increasingly encountering more sophisticated fraud techniques, such as deepfake content. In Ofcom's 2024 survey, 68% of users aged 16+ reported they had seen deepfake images, 60% videos, and 29% text-based deepfakes. Among those exposed, 45% said the content related to a scam or fraudulent advertisement. Age differences are notable: 33% of those exposed to scams aged 16–24 reported seeing scam-related deepfakes, compared to 54% of users aged 55 and over.[100] However, as Ofcom's survey groups children and adults over 18 together under the 16+ category, it is not possible to isolate findings specific to children within this data.

Further evidence suggests that children's confidence in navigating digital environments may not always align with their ability to detect online financial risks. While the previous data includes both children and young adults, further evidence suggests that overconfidence in digital skills among children may also contribute to increased vulnerability. Ofcom's 2022 media use report found that while children (aged 12-17) in England (74%), Wales (73%) and Scotland (78%) reported confidence in distinguishing real from fake content online, it also stated that children in England were more likely than those in Wales to pick any unreliable identifiers (83% vs 74%).[101] Ofcom's 2025 Children and Parents Media Use and Attitudes Report noted that there was a dip in confidence in the 2024 report among 16-17s who say they know how to distinguish between the real and the fake online content.[102] The 2025 report stated that this had been sustained: In 2022, 82% of 16-17s said they were confident in judging what is real or fake online, with this proportion falling to three-quarters in 2023 and remaining level this year.

Adults (18-65)

Fraud exposure continues into adulthood. A nationally representative survey conducted by Savanta for Citizens Advice in August 2024 found that 18% of UK adults aged 18 and over report experiencing at least one financial scam in the previous 12 months, based on a weighted sample of 2,117 respondents.[103] According to Ofcom (2024), adults aged 18–34 are significantly more likely than average to say they encounter content online they suspect to be a scam or fraud – 92% compared to

[97] Ofcom, 2024. Online Nation 2024 Report, p. 91.
[98] Nominet, 2023. Digital Youth Index 2023, p. 33.
[99] Vodafone Digital Parenting Team, 2023. Fastest growing group of online scam victims: it's teens, not seniors, Digital Parenting, Vodafone UK.
[100] Ofcom, 2024. Online Nation 2024 Report, p. 95.
[101] Ofcom, 2022. Children and Parents: Media Use and Attitudes Report 2022, p. 73
[102] Ofcom, 2025. Children and Parents: Media Use and Attitudes Report, p. 6.
[103] Citizens Advice, 2024. 9 million people caught out by financial scams in the past year.

the national average of 87%.[104] Nearly half (46%) of all adult internet users report personally engaging with scam or fraud content, and 39% know someone else who had been victimised.[105]

One study showed that adults under 55, particularly those aged 18-34, are disproportionately affected by a wide range of financial scams. Liverpool Victoria's Wealth (2024) reports that in the UK, 86% of the 3.8 million people who lost money to purchase scams in the past year are under the age of 55, with those aged 18-34 more likely than any other age group to experience and lose money to a range of financial scams, including refund, impersonation, investment, and purchase scams.[106] The findings also show that 36% of UK adults had experienced a trusted organisation scam in the previous 12 months, with a higher proportion of 18–34-year-olds affected across all fraud types named in the study.[107]

Survey data further highlight that adults aged 18–34 more likely than others to report higher rates of online fraud victimisation. This is shown in the data by Crest Advisory showing that adults aged 18–34 are substantially more likely to report having been victims of online fraud (32%) than those aged 35 and over (16%).[108] Notably, adults aged 18-34 were disproportionately affected by advance fee fraud, being three times more likely to fall victim than those aged 35 and over (18% vs. 6%).[109] National Fraud Intelligence Bureau data suggests that the average financial loss per report of advance fee fraud is £1,875, with the average age of victims being 18 years old.[110] Survey data from Goldman Sachs (2024) further highlight that financial scams are a significant concern among adults aged 18 to 34 in the UK.[111] The findings show that 17% of individuals in this age group report having lost money to fraud compared to 9% of those aged 55 and over. Additionally, 32% of 18 to 34-year-olds expressed feeling vulnerable to scams.[112] The survey also identifies several behavioural factors that may contribute to this vulnerability, including the sharing of login credentials, ignoring alerts about data breaches, and oversharing personal information on social media services. Importantly, 31% of 18 to 34-year-olds report ignoring a notification that their passwords have been involved in a data leak, compared to 19% of those aged 35 to 54 and 12% of those aged 55 and over. These behaviours increase the likelihood of encountering fraudulent financial content while searching for or engaging with financial services online.[113]

Survey data also suggest that adults aged 18–24 seem to be especially susceptible to impersonation scams, despite high levels of self-reported confidence in identifying scams. UK Finance's Take Five to Stop Fraud campaign highlights the heightened vulnerability of UK adults aged 18–24 to impersonation scams.[114] In their survey, 49% of respondents in the 18–24 age group report being contacted by an impersonation scammer, compared to 32.5% of those aged over 55.[115] Of those targeted, 52% of 18–24-year-olds admit to sharing personal information or making a payment

---

[104] Ofcom, 2024. Online Nation 2024 Report, p. 95.
[105] Ofcom, 2023. Online Scams & Fraud Research: Executive Summary, prepared by Yonder Consulting, p. 5.
[106] LV, 2024. Wealth and Wellbeing Research Programme: Financial Scams and Consumer Impact.
[107] LV, 2024. Wealth and Wellbeing Research Programme: Financial Scams and Consumer Impact.
[108] Crest Advisory, 2023. Online Fraud: What Does the Public Think?, Crest Advisory, citing data from Office for National Statistics, 2022, Nature of fraud and computer misuse in England and Wales: appendix tables.
[109] Crest Advisory, 2023. Online Fraud: What Does the Public Think?, Crest Advisory, citing data from Office for National Statistics, 2022, Nature of fraud and computer misuse in England and Wales: appendix tables.
[110] Crest Advisory, 2025. Understanding and addressing fraud against children and young people: An action plan, pp. 3–30.
[111] Marcus by Goldman Sachs, 2024. Fraud: what are the facts?.
[112] Marcus by Goldman Sachs, 2024. Fraud: what are the facts?.
[113] Marcus by Goldman Sachs, 2024. Fraud: what are the facts?.
[114] UK Finance, no date. Take Five to Stop Fraud Campaign Insights.
[115] UK Finance, no date. Take Five to Stop Fraud Campaign Insights.

as a result. While the campaign insights do not specify whether these scams occur online, the emphasis on digital confidence and behaviours, such as recognising fake requests for personal information, suggests that many of these interactions take place through digital or online services. Despite high levels of self-reported confidence in identifying scams (91%), only 27% of 18–24-year-olds say they always verify unexpected requests, compared to over 60% of those aged over 55.[116]

One study suggests that adults aged 55 and over seem to more frequently report exposure to scam-related deepfake content than those aged 18–24. Ofcom (2024) data reveal that, of those who have been exposed to a deepfake, people aged 55-64 and 65 and over are particularly exposed to deepfake scams, with over half reporting they have seen deepfake fraudulent or scam advertisement – far higher than adults aged 18-24.[117]

Adults (65+)

Adults in the UK, particularly those aged 65 and over, are identified in a 2021 policy briefing by UCL Dawes centre for Future Crime as being at greater risk of experiencing financial harm from online fraud and cybercrime.[118] Cybercrime includes consumer frauds and scams designed to obtain financial benefit by deceiving a victim, often directing them to harmful websites that download viruses or steal passwords, bank details, and other sensitive information.[119] The aforementioned policy briefing by UCL and a literature review by Burton et al related to older people and financial cyber crime attribute this heightened vulnerability to a mix of factors, including lower levels of digital literacy, age-related health conditions, and increased social isolation, all of which may make individuals more receptive to manipulative scam content.[120] [121]

A survey produced by Crest Advisory and a study by Low et al. caution against generalising risk across all individuals aged 65 and over. While sources identify heightened vulnerability among adults aged 65 and over, other research advises caution in making broad generalisations.[122] [123] The aforementioned survey conducted by Crest Advisory in 2023 found that adults, particularly those aged 55–64 (12%) and over 65 (13%), reported the lowest levels of victimisation in the past year.[124]

One study by Independent Age suggests that UK adults over 65 years old are frequently targeted by scams when seeking everyday financial services and information online. According to Independent Age, the most commonly reported scams among over-65s include retail or delivery fraud (43%), online shopping scams (30%), impersonation of HMRC (30%), and bank-related scams (28%).[125] These often arise while attempting to make legitimate payments, access pension or tax

---

[116] UK Finance, no date. Take Five to Stop Fraud Campaign Insights.
[117] Ofcom, 2024. Online Nation 2024 Report, p. 95
[118] UCL Dawes Centre for Future Crime, 2021. Older adults as victims of online financial crime, University College London, pp. 1–4.
[119] UCL Dawes Centre for Future Crime, 2021. Older adults as victims of online financial crime, University College London, pp. 1–4.
[120] Burton, Amy; et al, 2022. Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review, Experimental Gerontology, 159, 111678.
[121] UCL Dawes Centre for Future Crime, 2021. Older adults as victims of online financial crime, University College London, pp. 1–4.
[122] Crest Advisory 2023. Online fraud: What does the public think?.
[123] Low, Natalie; and Lally, Clare 2024, Social and psychological implications of fraud, POSTnote 720, UK Parliament, published 29 April 2024, pp. 1–19
[124] Crest Advisory, 2023. Online Fraud: What Does the Public Think?, Crest Advisory, citing data from Office for National Statistics, 2022, Nature of fraud and computer misuse in England and Wales: appendix tables.
[125] Independent Age, 2024. The hidden cost of scams: Understanding the lasting impact of financial fraud on older people and vulnerable customers, pp. 5-20.

information, conduct online banking, or engage in routine consumer transactions such as parcel delivery re-bookings or service cancellations. Several victims reported being defrauded while attempting to obtain customer support or information – e.g., being misdirected to fake Citizens Advice or product help pages through online search results.[126]

Social media and marketplace platforms are mentioned in cases involving scams related to companionship and consumer goods. A popular marketplace service that also has a social media function was cited in responses to interviews conducted by Re-engage in 2023, where victims were targeted after expressing interest in companionship or consumer goods.[127] Fake financial services, such as investment schemes, cryptocurrency offers, or "get rich quick" ads, were also reported.[128]

Fraud tactics targeting adults aged 65 and over include impersonation, automation, and emerging AI-based techniques. While perpetrators are often anonymous, the tactics suggest a combination of organised crime groups using spoofing, a technique through which a cybercriminal disguises themselves as a known or trusted source[129], and automation tools, as well as opportunistic actors exploiting search and communication services.[130] Independent Age flagged the emerging role of AI-generated deception, including deepfake videos and voice cloning, which have begun to appear in phishing content.[131] An AI tool reportedly available on the dark web which enables users to generate automated scam content was cited by Independent Age as an example of automated scam content generation.[132]

Some evidence examined suggests low accuracy in scam recognition among adults aged 65 and over. Although many claim confidence in identifying scams, in one Independent Age study 55% of over-65s failed to correctly judge whether a test message from their bank was genuine.[133] In a different study by Re-Engage, individuals reported their confidence to be especially low in identifying scams via websites and social media.[134] Research by Ofcom showed that older age groups (65+) were better able to identify a form of fraud than younger adults.[135]

Financial and emotional consequences have been documented among adults aged 65 and over. Evidence from Independent Age suggests that 17% of over-65s have been defrauded, losing an average of £3,799 each,[136] with the same study and another conducted by Re-engage highlighting that many cases going unreported due to confusion, shame, or low digital confidence.[137] [138] Research

---

[126] Independent Age, 2024. The hidden cost of scams: Understanding the lasting impact of financial fraud on older people and vulnerable customers, p. 7
[127] Reengage, 2023. The unseen price of a scam: Impact of scams and fraud on isolated older people, pp. 1–16.
[128] Independent Age, 2024. The hidden cost of scams: Understanding the lasting impact of financial fraud on older people and vulnerable customers, p. 8
[129] Joshua, Crissy, 2024. What Is Spoofing? How to Protect Yourself with 12 Different Examples, Norton Blog.
[130] Independent Age, 2024. The hidden cost of scams: Understanding the lasting impact of financial fraud on older people and vulnerable customers, pp. 1–4
[131] Independent Age, 2024. The hidden cost of scams: Understanding the lasting impact of financial fraud on older people and vulnerable customers, pp. 1–4
[132] Independent Age, 2024. The hidden cost of scams: Understanding the lasting impact of financial fraud on older people and vulnerable customers, p. 18.
[133] Independent Age, 2024. The hidden cost of scams: Understanding the lasting impact of financial fraud on older people and vulnerable customers, p. 8.
[134] Reengage, 2023. The unseen price of a scam: Impact of scams and fraud on isolated older people, p. 6.
[135] Ofcom, 2025. Adults' Media Use and Attitudes Report, p. 18.
[136] Independent Age, 2024. The hidden cost of scams: Understanding the lasting impact of financial fraud on older people and vulnerable customers, pp. 5–20
[137] Independent Age, 2024. The hidden cost of scams: Understanding the lasting impact of financial fraud on older people and vulnerable customers, p. 13.
[138] Reengage, 2023. The unseen price of a scam: Impact of scams and fraud on isolated older people, p. 7.

from Re-engage suggests that a fear of scams also led to withdrawal from online services altogether.[139]

Repeat victimisation and ethnicity-related disparities are observed among adults aged 75 and over in the literature examined. Findings from a probability sample survey in England and Wales conducted by Havers et al highlights ethnicity-related disparities in victimisation risk.[140] According to the UCL Dawes Centre for Future Crime, this pattern suggests that the scams targeting adults in this age group may be more severe in nature, and that under-reporting, possibly driven by shame or fear of losing independence, may obscure the true extent of financial harm, particularly in cases of online fraud and cybercrime. [141] The study by Havers et al also highlights ethnicity-related disparities in victimisation risk. Adults aged 75 and over from Black, African, Caribbean, or mixed ethnic backgrounds were more likely to experience cybercrime than white people, whereas those of Asian or Asian British ethnicity were less likely to be victimised.[142]

Common themes across age groups

Some recurring themes and developments emerge from the current literature on how fraud, often facilitated by disinformation, and contribute to financial harm in the UK, particularly across different age groups.

Overconfidence in fraud detection is noted across age groups. Despite high levels of self-reported confidence, individuals across age groups often fail to take protective actions or accurately identify fraud. A survey by Independent Age showed that among adults aged 65 and over, 55% misjudged a test message from their bank[143], while a separate study reports that only 27% of 18–24-year-olds say they always verify unexpected requests, compared to over 60% of those aged over 55.[144] A survey conducted by Ofcom in 2022 revealed children aged 12–17 also reported confidence in spotting fake content online, yet many selected unreliable indicators when tested.[145] Ofcom's 2025 Adult's Media Use and Attitudes report noted an increase in the 'confident and not able' group with 4% of internet users confident in their ability to recognise scams but who did not respond appropriately in the email scam scenario this year, compared to 12% last year.[146] Those more likely to be in this category are those aged 16-24 (19%) or 25-34 (27%), men (16%) and those in social grade ABC1 (15%).

Age-Related vulnerabilities are complex and evolving. Although the available literature significantly covers children and adults over 65, it also reveals that adults aged 18–34 are disproportionately affected by a range of online fraud. This group is highly digitally active and reports high confidence in identifying scams; however, this confidence does not consistently translate into cautious behaviour, as only 27% of 18–24-year-olds say they always verify unexpected requests, compared to over 60% of those aged over 55.[147] Conversely, research by both Independent Age and Havers et al. says adults

---

[139] Reengage, 2023. The unseen price of a scam: Impact of scams and fraud on isolated older people, pp. 1-16.
[140] Havers, B.; Tripathi, K.; Burton, A.; McManus, S., and Cooper, C., 2024. Cybercrime victimisation among older adults: A probability sample survey in England and Wales, PLoS ONE, 19:12, pp. 1–10.
[141] UCL Dawes Centre for Future Crime, 2021. Older adults as victims of online financial crime, University College London, pp. 1–4
[142] Havers, B.; Tripathi, K.; Burton, A.; McManus, S., and Cooper, C., 2024. Cybercrime victimisation among older adults: A probability sample survey in England and Wales, PLoS ONE, 19:12, pp. 1–10.
[143] Independent Age, 2024. The hidden cost of scams: Understanding the lasting impact of financial fraud on older people and vulnerable customers, p. 8.
[144] UK Finance, no date. Gen Z more likely to be tricked by criminals and fall for impersonation scams.
[145] Ofcom, 2022. Children and parents: media use and attitudes report 2022, p. 73.
[146] Ofcom, 2025. Adults' Media Use and Attitudes Report, p. 18.
[147] UK Finance, no date. Gen Z more likely to be tricked by criminals and fall for impersonation scams.

(over 65) may be less frequently targeted but are more likely to suffer repeat victimisation and higher financial losses.[148] [149] Studies by the Children's Society and Parent Zone suggest that children are increasingly exposed to scams through gaming services, with limited institutional recognition of these risks.[150] [151]

[148] Independent Age, 2024. The hidden cost of scams: Understanding the lasting impact of financial fraud on older people and vulnerable customers, pp. 5–20.
[149] Havers, B.; Tripathi, K.; Burton, A.; McManus, S., and Cooper, C., 2024. Cybercrime victimisation among older adults: A probability sample survey in England and Wales, PLoS ONE, 19:12, pp. 1–10.
[150] The Children's Society, 2025. Moving Money, pp. 3–30.
[151] Parent Zone, 2025, Short Changed and Out of Time: A Report into Families Facing Financial Harms Alone, p. 12.

Cross-cutting points and summary

Limitations and future research directions

This review focuses on the most recent and pertinent material, prioritising sources that directly address the intersection of fraud and disinformation in the UK context.

A key limitation lies in the inconsistent use of terminology across the literature. Terms such as fraud, scam, and disinformation are often used interchangeably, making it difficult to distinguish between different types of financial deception and their specific mechanisms. This lack of definitional clarity complicates the synthesis of findings.

The review does not examine literature that addresses the consequences of financial harm in detail. Although there is literature addressing the outcomes experienced by different age groups, this review does not systematically explore the psychological, social, or economic impacts of financial deception. Future research could usefully investigate these consequences to provide a fuller understanding of the significance of online financial harm and the importance of protective measures.

Additionally, the segmentation of age groups across the literature presented analytical challenges. Many sources do not disaggregate data in a way that aligns with the review's age bands (under 18, 18–65, and over 65). For instance, many findings use open-ended age brackets such as '55 and over' without specifying an upper boundary, making it unclear whether the data primarily reflects those aged 55–75 or includes individuals aged 75 and over. This ambiguity limits the precision of age-specific analysis and may affect the interpretation of risk across demographic groups.

Summary

This literature review has identified literature about how individuals across different age groups access financial information online, how they might experience fraud using financial disinformation, and highlighted how they may experience age-related vulnerabilities. The evidence examined in this review indicates that financial deception is widespread and multifaceted, affecting individuals across all age groups, though the nature and severity of harm vary significantly.

Children and adolescents are increasingly exposed to fraud through gaming and social media services, often in environments that normalise spending and lack adequate safeguards. Despite growing digital awareness, users aged 12-17 overestimate their ability to detect fraud, while professionals and institutions are often reported to be underprepared to identify and respond to financial exploitation in this age group.

Among adults aged 18 to 34, the literature identifies a high level of exposure to online financial fraud, including impersonation, investment, and purchase fraud. This group is particularly vulnerable due to behavioural factors such as oversharing personal information and ignoring security alerts, despite reporting high confidence in their ability to identify fraud. Adults in this age range are also more likely to suffer financial loss than adults over 65.

Older adults, particularly those over 65, face distinct risks. While some literature reports that they may be less frequently targeted, they are more likely to experience repeat victimisation and higher

financial losses. Factors such as lower digital literacy, social isolation, and health-related vulnerabilities contribute to their susceptibility. However, the literature also cautions against overgeneralising these risks, noting that adults over 65 are not uniformly more vulnerable than other age groups.

Across all demographics, the consequences of financial harm extend beyond monetary loss, encompassing emotional distress, social withdrawal, and long-term behavioural changes. The review also highlights gaps in institutional responses, inconsistencies in age segmentation across data sources, and a lack of clarity in terminology, all of which may limit the effectiveness of current interventions.

Addressing these challenges will require more precise definitions, improved demographic data, and targeted research into the lived experiences and consequences of financial harm of different groups.