Online Information Advisory Committee

# Understanding Online Financial Harm

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

27 November 2025

# Background

This is the first report of a series of advice notes published by Ofcom's Online Information Advisory Committee ('the Committee'), a body established under Section 152 of the Online Safety Act. The Committee's function is to provide independent advice to Ofcom about: how providers of regulated services should deal with disinformation and misinformation on such services, and the exercise of certain powers and duties, as they relate to disinformation and misinformation on regulated services.[1]

The Committee's approach is grounded in fundamental rights, particularly the right to freedom of expression under Article 10 of the Human Rights Act.

The aim of the Online Safety Act regime is to reduce harms suffered by people in the UK when they are online. The Committee's work reflects this scope, and any advice should be read as relating to UK users. The Committee's work covers areas where the harms relate to the production and distribution of false and misleading information, as outlined under the UK's Online Safety Act. This is a field of diverse potential harms. The Committee's work will look at a series of specific areas of harm and provide advice in relation to them.

The first report focuses on the area of online fraud where people are exposed to financial loss after exposure to false or misleading information. The National Security Strategy (2025) estimates the total cost of fraud against individuals in the UK at a minimum of £6.8 billion. Nearly nine in ten UK adult internet users (87%) report encountering material they believe to be fraudulent or part of a scam. Fraud remains one of the most significant threats to individuals and the UK economy and therefore is an appropriate harm for the Committee's first advice note.

The Committee asked Ofcom to collate relevant literature to understand the different ways disinformation is used to deceive people for the purpose of defrauding them online and considered the demographics of those likely to be affected. Ofcom also brought together information about existing laws and regulation. The Committee is publishing the literature review associated with this report so that readers can better understand the rationale for the recommendations laid out below.

The members of Ofcom's Online Information Advisory Committee wrote this report independently, drawing on the literature review and their own relevant expertise.

Further information about our methodology can be found in the literature review published alongside this report.

This report is divided into four sections. The first outlines how harms can manifest from such content online. The second maps how these harms are distributed across age groups. The third assesses existing legal and regulatory tools for confronting these harms. The fourth presents the committee's recommendations to Ofcom on how to confront these challenges while upholding individuals' rights.

[1] This includes Ofcom's transparency powers under Section 77 of the Online Safety Act, and Ofcom's media literacy functions under Section 11 of the Communications Act 2003.

# How this harm manifests online

What is fraud?

Fraud includes a range of different offences, including:

- Fraud by false representation
- Fraud by abuse of position and participating in fraudulent business carried on by sole trader etc.
- Fraud related to misleading statements or impressions about investments
- Offences related to articles for use in fraud

## Online fraud: Content types and distribution mechanisms

People in the UK can experience fraud in a range of settings, online and offline, and in a wide variety of formats. False or misleading financial information plays an important role as a mechanism through which people may become vulnerable to fraud. Email and telephone are among the most reported delivery methods for fraud. It is important there is also a focus on these other delivery methods. But this report focuses on online forms of communication within the scope of Ofcom's online safety responsibilities. The main types of online fraud in this report are:

- Counterfeit or spoofed websites, often involving the imitation of legitimate services or trusted institutions to exploit a victim's trust.
- Impersonation fraud (including the impersonation of official bodies), often falsely claiming to be a trusted organisation or individual to persuade victims to share personal or financial information or make payments.
- Loan fee fraud, such as where fraudsters ask for a fee for a fake loan, falsely claiming it is refundable.
- Counterfeit good scams where a fake product is sold as authentic.
- Investment, pension, or "get rich quick" scams, typically involving high-risk financial schemes falsely presented as lucrative opportunities or involving a fake investment.
- Fake employment scams.
- Identity fraud, including where someone pretends to be the victim and may gain access to personal information through misleading information.
- Fake holiday bookings, where someone pays money for holiday rent online where all, or parts, of the holiday do not exist.
- False or deceptive debt advice.
- Activity that overlaps with other forms of harm, such as the use of ransomware scams or phishing. In these instances, fraud is one part of the activity.

Fraud increasingly occurs across a wide range of online services. Services with high volumes of peer-to-peer interaction, such as social media, messaging apps, and marketplaces, are reported to be more fertile ground for fraudsters because of the greater ability to engage directly with people located in the UK. The emergence of AI-generated content adds another layer of complexity and risk for consumers navigating digital spaces.

Creating fake user profiles on a user-to-user service enables fraudsters to commit or facilitate fraud. It allows them to conceal their identity and impersonate legitimate entities such as banks, insurance providers or financial advisors to add legitimacy to false claims. Fraudsters can also use people who have many user connections to achieve their aims, while user groups can be used by fraudsters to share knowledge to successfully carry out scams.

Because the types of services that users engage with vary based on age and other characteristics of the user, the risk levels of different service types for false or misleading financial information can vary depending on the demographic factors of its users, such as age.

Risk levels also vary by how people use those services, such as by the financial products they look for across social media, messaging apps and online marketplaces. More information related to these differences can be found in the section on existing research.

## Online fraud: Actor types

It is helpful to summarise the types of actors who may be responsible for particular types of harm.

From the literature reviewed, the three groups described below provide a framework for characterising the range of actors involved in harmful or deceptive activities in the context of false or misleading financial information. This classification also offers a practical basis for organising evidence on observed behaviours. These groups are not mutually exclusive and may overlap, nor can they always be precisely defined.

- **Direct individual actors** – such as some financial influencers using deceptive information, impersonators, money mule recruiters, or independent scammers acting knowingly and with intent to cause harm. Some deceptive financial influencers operate on popular social media services to promote unauthorised or non-existent financial products,[2] while portraying themselves as credible experts. These are the most prominent actors in this category. But it can also include those involved in impersonation fraud, unauthorised investment offers, and others involved in financial deception.
- **Direct group actors** – such as organised fraud organisations and coordinated influence networks operating collectively. Unlike the previous category, these actors orchestrate their activity across networks of digital infrastructure and human actors. They often mirror legitimate commercial or financial activity making their activity difficult to determine as illegitimate. They rely on persuasive language to appeal to victims. Examples include consumer investment fraud, employment fraud, and the use of cloned websites.
- **Indirect/intermediate actors** – such as affiliate marketers, exploitative intermediaries, or people who contribute to the spread of fraudulent content through mechanisms such as fake endorsements or clickbait. They may, or may not, be fully aware of their role in fraud

[2] 'A product that is connected to the way in which you manage and use your money, such as a bank account, credit card, insurance etc.' Cambridge Dictionary, no date. Financial product. [accessed 12th September 2025]

ecosystems. In many cases, these are third parties who are inadvertently involved in the dissemination of fraud.

These groups often target, or contribute to the targeting of, their content and activity at a particular group of people in the UK or to a specific type of online service.

## Online Harm: Victim types

Anyone in the UK can potentially be exposed to and experience harm from fraud enabled by false or misleading financial information. The literature identifies risk factors such as low levels of conscientiousness, higher impulsivity, cognitive decline and social isolation.

Research into the risks faced by socio-demographic groups points to elevated risks for some groups including women, individuals in higher income or education brackets, single parents and LGBTQ+ individuals.

Similarities and differences across age groups are outlined in more detail in the table below. Outline of research examined in the literature review:

| Children | Adults aged 18-65 | Adults aged 65 and over |
|---|---|---|
| • Evidence shows that children can face risks of financial harms in online environments, with financial losses among those under 13 and adolescents observed beyond the UK.<br>• Two studies suggest financial risks to children online remain under-recognised. Evidence also highlights emerging patterns of financial exploitation of children, identified as a developing form of abuse.<br>• Research examined also highlights the emergence of more | • Fraud exposure persists into adulthood, according to several sources.<br>• One study shows that adults under 55 were disproportionately affected by a wide range of online scams, and survey data highlights that adults aged 18-34 more likely than others to report higher rates of online fraud victimisation.<br>• Another study suggests that adults aged 55 and over reported being slightly less likely to see deepfakes, but of the deepfakes[3] they saw a higher proportion | • One policy briefing identifies this group as being at heightened risk of financial harm from online fraud and cybercrime<br>• Two sources caution against over-generalising risk across all individuals aged 65 and over.<br>• Social media and marketplace platforms are mentioned in cases involving scams related to companionship and consumer goods in evidence examined.<br>• Sources indicate that fraud tactics targeting this group include impersonation, |

[3] 'Deepfakes are audio-visual content that has been generated or manipulated using AI, and that misrepresents someone or something.' Ofcom, 2024. Deepfake Defences: Mitigating the Harms of Deceptive Deepfakes.

| | | |
|---|---|---|
| sophisticated fraud techniques.<br>• Further evidence suggests children's confidence in in using digital environments may exceed their actual ability to detect fraud or deception | were scam-related deepfakes compared to other age groups. | automation and emerging AI-based techniques.<br>• Some evidence examined points to low accuracy in scam recognition among adults in this age group<br>• Financial and emotional consequences have been documented among adults aged 65 and over in two studies.<br>• Repeat victimisation and ethnicity-related disparities are observed among adults aged 75 and over in the literature examined. |
| **Common themes across age groups** | | |
| • Overconfidence in fraud detection is noted across age groups in the literature examined.<br>• Sources explored suggest age-related vulnerabilities are complex and evolving. | | |

*The above table summarises the literature review which informed this note. More detail can be found in the full literature review here.*

## Children

Based on the literature review, financial risks to children may be under-recognised. The research attributes this risks to assumptions that children are not active financial agents or that sums involved are too minor to warrant serious concern. Emerging evidence contradicts this assumption. One in five of UK parents report their child had encountered a money-related problem online in a study conducted in 2025. Another report highlighted financial exploitation of children as an emerging and under-recognised form of abuse.

The collective literature review demonstrated children of different age groups reported experiencing scams, including children as young as 8 years old. Other data suggested teenagers were one of the fastest online growing cohorts of online scam victims.

Research from the UK Safer Internet Centre showed children are exposed to scams most commonly through social media, followed by email and online games. This research also suggests the most

common scam types experienced by children include fake giveaways, phishing scams, fake websites, online shopping scams, and trust trades in online games. Other research also highlights the emergence of more sophisticated scams, including deepfakes.

## Adults aged 18-65

Ofcom's Online Experiences Tracker shows nearly half of all adult internet users report personally engaging with scam or fraud content, and 39% of those surveyed knew someone else who had a victim of this illegal behaviour.

A study from Crest Advisory suggests that adults aged 18-34 are affected by scams at higher rates than other adult age groups. In this research, the pattern was apparent across different types of scams, including, financial scams, refund scams, investment scams, impersonation scams and purchase scams. Survey data also highlights that adults aged 18-34 were more likely than others to report higher rates of online fraud victimisation.

In contrast, Ofcom's data show that adults 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.

## Adults aged 65 and over

The literature review is inconsistent about whether adults aged 65 and over are more at risk of harm from false or misleading financial information than other age groups. Like other age groups, several studies show that adults aged 65 and over report encountering scams online. The types of scams reported include retail or delivery fraud; online shopping scams; impersonation of HMRC; bank-related scams and fake financial service scams. Other research highlights the emerging role of AI-generated deception in this age group's experience. That includes the use of deepfake videos and voice cloning in phishing content, and for the automated generation of scam content. Research by Ofcom showed that older age groups (65+) were better able to identify a form of fraud than younger adults.

A study by Independent Age highlights the common scenarios in which adults over 65 experience scams. These include when they are making transactions, accessing pension or tax information, conducting online banking and accessing customer support.

Several pieces of research show the negative impacts of scams on this age group. This includes financial loss (one study reported that over 65s who are defrauded lose an average of £3799 each) and withdrawal from online services. A study by the UCL Dawes Centre for Future Crime also suggests that adults over 65 under-report these impacts. Reasons for this include embarrassment, low digital confidence, and fear of losing independence due to others potentially perceiving this as a decline in their ability to care for themselves. The same study suggests that the true extent of financial harm, particularly from online fraud and cybercrime, may be obscured in this age group.

## Commonalities and differences

All age groups are exposed to false or misleading financial information as a tactic to enable forms of fraud. But a full understanding of how age affects this vulnerability is complex, evolving and, currently, unclear. For example, the literature review showed that 18–34-year-olds are disproportionately affected by a range of online fraud types, but adults over 65 are more likely to suffer repeat victimisation and higher financial losses. Studies by the Children's Society and Parent

Zone suggest limited institutional recognition of these risks to children, despite evidence of their exposure to this type of harm.

Understanding the reasons behind these trends is complex. Across age groups, the literature review suggests some people are over-confident in their ability to identify this type of harm.

There is a growing recognition in the literature that harm extends beyond financial loss. It can also be emotional and psychological. The literature review suggests impacts from false or misleading financial information are likely under-reported, and there are institutional gaps in awareness and response to this type of harm.

There are limitations in the evidence base which informs these findings. These include:

- In the literature, key terminology is used interchangeably with limited consistency in definitions. This can make it challenging to distinguish between different forms of financial deception and respective mechanisms of harm.
- Many sources do not use the same age bands as the ones this note, and literature review are organised into. Some use open-ended age bands, and across the literature there is little consistency in the age bands measured. In some cases, we have had to make inferences based on all these datasets. This may impact the representativeness of our conclusions about risk of harm.
- The literature review does not detail all the consequences of financial harm and have not systematically explored the psychological, social or economic impacts of fraud facilitated through financial deception.
- The literature review primarily uses the lens of age to explore experiences of social engineering through financial disinformation for the purpose of fraud. It is not the only factor in determining exposure to, or experience of harm from, such content. As highlighted, false or misleading financial information may have a disproportionate impact on vulnerable or marginalised groups to a greater extent as the result of other factors and characteristics.
- Across the literature review, the level of harm is likely to be under-reported by some groups, potentially affecting the representativeness of conclusions.

# Existing law and regulation

There is a variety of legal and regulatory regimes designed to address the harms discussed in this report.

Much of this harmful content would be in breach of criminal law in the UK. Such offences can be prosecuted by law enforcement, and regulatory actions may be taken by financial regulators or trading standards authorities.

Specific fraud offences are included as priority offences under the Online Safety Act. All providers of in-scope services must assess the risk of those offences taking place on their services. They must put in place appropriate systems and processes to prevent users from encountering such content. Ofcom is the independent regulator enforcing the Online Safety Act. While it does not have a role in acting on individual pieces of content, regulated services must enable users to report suspected fraudulent user-generated and search content to them.

Some providers of regulated services have included provisions in their terms of service designed to address forms of fraudulent content. The Online Safety Act also requires firms include provisions in their terms of service specifying how individuals are to be protected from content that breaches UK law, including the Fraud Act. The Online Safety Act gives separate duties to categorised services to tackle fraudulent content in online adverts. Ofcom aims to consult on its Code of Practice on how such services should meet these duties around July 2026. Outside of its online safety work, Ofcom also carries out work in relation to fraud and scams in telecommunications services.

Other regulators have a significant role in this space.

The CAP Code, which is enforced by the Advertising Standards Authority (ASA), places specific requirements on advertisers in relation to the recognition of advertising, misleading advertising, and advertising of financial products.

Trading Standards acts as a legal backstop to the ASA's enforcement of misleading advertising in the non-broadcast space.

The Competition and Markets Authority enforces against breaches of consumer protection law, which extends to advertising. It has collaborated with the ASA on awareness campaigns in relation to compliance of influencer advertising with relevant rules.

There are specific rules for providers of financial products and services that are enforced by bodies like the Financial Conduct Authority (FCA). In November 2024, the UK Government confirmed it would proceed with legislation to bring certain crypto assets activities into the FCA's regulatory perimeter.

# Conclusions

Our recommendations to Ofcom are as follows:

- The new requirements in the Online Safety Act related to illegal fraudulent content should make a material difference to the exposure of people in the UK to this class of harmful material. Ofcom should develop a plan to collect data and evaluate measures related to fraud to aid the understanding of their effectiveness.
- The Committee is concerned that risk of false or misleading financial information targeting children may be under-recognised, based on the literature review, and would like to see this considered fully in the development measures to protect children.
- Some types of harmful activity associated with online fraud will not meet the definition of criminal fraud. But they may contravene the terms of service of online services. Where Ofcom has powers to engage with services around user reporting and enforcement of terms of service, it should ensure this engagement covers these activities.
- Ofcom should also recommend best practices for addressing the barriers identified in this report, for example, ensuring reporting interfaces are accessible and intuitive across all service types, including social media, messaging apps, marketplaces, and gaming services. The design of online services will shape the interactions between fraudsters and their victims, as well as the extent to which people are exposed to harms. Where increased risk is associated with specific design features, including services' recommender systems, Ofcom should engage with services to mitigate these harms.

- The Committee's analysis shows the broad range of risks people face, which are expected to continue to evolve at pace. Ofcom should consider how it can make sure it is adequately prepared to respond to emerging and fast-evolving harms. The risk assessments that online services are required to provide to Ofcom should be a useful source of information.
- We recommend that Ofcom encourage platform providers to offer age-appropriate educational messaging that reflect differences in how users across age groups encounter and respond to potentially false or misleading financial information. For children, warnings should be clear and informative without causing unnecessary concern; for adults aged 18–34, messaging can address common overconfidence in fraud detection; for adults over 65, communications should be accessible and respectful to support reporting and maintain digital confidence.
- Ofcom has an established process for working with other UK regulators. The cross-cutting nature of financial harms makes it a good test case for that co-operation within the digital sphere. Joint work to look at the intersection of online safety, data protection, and financial services regulation would help with understanding how these regimes can be made to work together in the public interest to mitigate against false or misleading financial information. As part of this initiative, it is recommended to evaluate potential barriers and solutions that address risks spanning multiple regulatory areas in the UK. For example, measures to prevent impersonation of legitimate financial institutions could reduce harm across different domains.
- Future studies should aim to clarify terminology, improve the granularity of demographic data, and explore the lived consequences of financial harm that extends beyond monetary loss by different groups. Comparative evidence from international contexts may also offer valuable insights to understand and strengthen protections against false or misleading financial information in the UK.