the payments association

The new origin of APP fraud:

Evidence of digital platforms' role and the case for shared accountability

How digital platforms facilitate scam exposure and why accountability should be shared across the fraud chain

the payments association

Contents

Introduction

Authorised push payment (APP) fraud remains one of the most significant threats to consumers in the UK and Europe. In many cases, APP fraud originates well before any payment is initiated, with scams often beginning on social media, messaging platforms, or online marketplaces. In 2024, £450.7 million was lost to APP fraud in the UK,[1] with £257.5 million recorded in the first half of 2025 alone.[2] Across the EEA, fraudulent credit transfers are estimated to total between €2.2 and €2.5 billion annually.[3]

These figures reflect more than aggregate financial losses. APP fraud frequently leads to the depletion of household savings, working capital losses for small businesses, and wider economic harm arising from reduced consumer confidence. The effects of these scams often extend beyond the point of payment, with victims experiencing prolonged financial, operational, and, in some cases, emotional impacts.

Where scams begin

In most cases, scam exposure occurs online. Victims frequently first encounter fraudulent advertisements, marketplace listings, or messages on digital platforms long before any payment instruction reaches the banking system. In the first half of 2025, 66% of reported cases began on online platforms, including social media and messaging services, while a further 17% began on telecommunications channels.[4]

Industry reporting further indicates that fraud exposure is concentrated within a small number of digital platforms. Analysis of consumer fraud reports by members of The Payments Association (TPA) reveals that Meta-owned platforms account for a disproportionately large share of APP fraud reported globally.

Interviews with TPA members reveal a consistent pattern. Scam journeys often begin through sponsored advertising or online marketplace listings, then migrate to private messaging platforms such as WhatsApp or Telegram, for more personalised manipulation and social engineering before payments are finally executed.

Mandatory reimbursement requirements introduced in October 2024 strengthened consumer protection at the point of payment. However, these rules operate at the final stage of the fraud lifecycle. In many cases, the initial exposure to the scam occurs earlier on digital platforms, outside the banking system.[5]

1 *UK Finance, 'Fraud continues to pose a major threat with over £1 billion stolen in 2024' (press release, 28 May 2025), "Authorised Push Payment fraud losses" section, https://www.ukfinance.org.uk/news-and-insight/press-release/fraud-report-2025-press-release (accessed 2 March 2026).*
2 *UK Finance, 'Over £600 million stolen by fraudsters in first half of 2025' (press release, 24 October 2025), "Authorised Push Payment fraud losses" and "Authorised Push Payment enablers" sections, https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps600-million-stolen-fraudsters-in-first-half-2025 (accessed 20 February 2026).*
3 *European Banking Authority and European Central Bank, '2025 report on payment fraud' (December 2025), Key findings and Section 2 (Levels of payment fraud), credit transfers totals and losses (EUR 2.5bn fraudulent credit transfers; EUR 2.2bn credit transfer losses), https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202512.en.pdf (accessed 15 March 2026).*
4 *UK Finance, 'Half Year Fraud Report 2025', https://www.ukfinance.org.uk/system/files/2025-10/Half%20Year%20Fraud%20Report%202025_0.pdf (accessed 5 March 2026).*
5 *Payment Systems Regulator, 'APP scams reimbursement' (policy and requirements, includes start date 7 October 2024 and scope), https://www.psr.org.uk/authorised-push-payment-scams/app-scams-reimbursement/ (accessed 5 March 2026).*

Where responsibility sits

This paper highlights a critical disconnect in the current fraud prevention framework. While financial institutions are responsible for detecting suspicious transactions and reimbursing victims, initial exposure to these scams often occurs outside the banking system, on digital platforms and messaging services.

This creates a mismatch between who is held responsible and where the scam actually begins.

This white paper examines whether current UK and EU accountability frameworks reflect how APP fraud develops in practice. As scam exposure increasingly occurs on digital platforms, policymakers are beginning to scrutinise the role of platforms in fraud prevention and whether responsibilities across the fraud chain should evolve.

This paper argues that responsibility for tackling APP fraud must extend beyond banks to the digital platforms where many scams begin. It calls for regulators to introduce enforceable standards for scam advertising, platform accountability, and cross-sector intelligence sharing.

Regulatory implications and desired outcome

The evidence in this paper indicates that incentives to improve consumer protections and fraud prevention are misaligned across the fraud chain. Payment service providers face direct reimbursement obligations, while major upstream digital platforms, particularly social media platforms, still do not face equivalent enforceable obligations when scam exposure occurs on their services.

This paper supports a shift from voluntary platform commitments to mandatory, enforceable standards for fraud prevention across advertising and messaging environments, with credible regulatory oversight and penalties for systemic non-compliance.

This is not proposed as retrospective punishment. It is proposed as a mechanism to create real incentives to tackle fraud at source, thereby protecting consumers worldwide.

Methodology and the evidence base

This white paper draws on publicly available quantitative data, policy and regulatory publications, investigative reporting, and qualitative interviews with industry stakeholders. Key sources include reporting from UK Finance and the Payment Systems Regulator (PSR), research on scam advertising exposure across digital platforms, and analysis of platform governance and advertising moderation practices. Together, these sources provide evidence on fraud incidence, loss values, scam exposure pathways, and the regulatory framework for preventing fraud.

Interview evidence is used in this paper to illustrate operational patterns observed across the fraud chain, rather than serving as the sole basis for its conclusions. The core analysis is supported by triangulation across public datasets, regulatory reporting, government publications, investigative reporting, and institution-level fraud data.

This distinction matters because no single dataset captures the entire scam journey. Taken together, however, these sources point to a consistent conclusion: scam exposure frequently occurs upstream within digital platform environments before financial institutions can intervene.

This paper does not seek to attribute sole causation of APP fraud to any single actor within the fraud chain. Fraud is typically a multi-stage process involving exposure, manipulation, and payment execution across different sectors. However, large volumes of scam exposure occur on digital platforms, and those platforms exercise substantial operational control over the environments in which fraudulent content is distributed.

In policy terms, the central issue is not sole causation, but whether platforms operate systems that enable large-scale exposure to scams and therefore have the capability to mitigate those risks. The evidence presented in this paper indicates that many scam journeys begin within platform-controlled advertising, marketplace, and messaging environments before any payment instruction reaches the banking system.

Member interviews

The Payments Association conducted a series of interviews, involving stakeholders in retail and SME banking, payment processors, financial crime intelligence providers, and fraud prevention technologies.

These interviews took place between January and February 2026, focusing on fraud prevention, the pathways of scam exposure, platform exposure dynamics, and cross-sector intelligence sharing.

All interview quotations were reviewed for accuracy before publication.

The following members of The Payments Association were interviewed for this paper:

- Allica Bank
- Allpay
- Ask Silver
- AVIEL Intelligence
- Barclays
- LSEG Intelligence
- Nationwide
- Revolut
- Santander UK
- Tide

Linking exposure to APP outcomes

The white paper distinguishes between:

- Scam exposure
- Victim manipulation
- Payment execution
- Financial loss

APP fraud typically unfolds through several stages: scam exposure, victim manipulation, payment execution, and eventual financial loss.

Victim-report origination data

Reported platform origination data is often sourced from customer testimony from fraud investigations. Financial institutions may not have independent access to upstream communication or advertising interaction records.[6]

Platform origin data should be interpreted in the context of known reporting limitations, which may vary in accuracy or completeness. Moreover, classification practices may differ across institutions, and some scam interactions occur through undocumented voice or video communication channels.

Despite these limitations, cross-institution reporting consistently indicates that scam activity often begins before any interaction with the banking system. Previous work by the Payments Systems Regulator (PSR) to develop a methodology for measuring scam origination highlights both the importance of this data and the challenge of achieving consistent, industry-wide adoption.[7]

Safeguards and independence

To strengthen the evidential basis of the analysis:

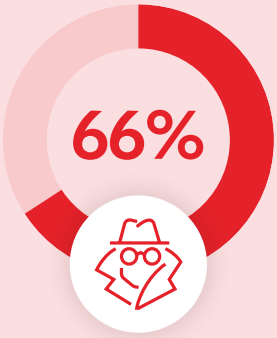
- TPA member interviewees were drawn from multiple sectors
- Both retail and SME banking perspectives were included
- Intelligence providers and payment processors were consulted
- Interview findings were triangulated against published datasets where available

6 *Home Office, Fraud Strategy 2026–2029 (March 2026), section describing establishment and funding of an Online Crime Centre, https://assets.publishing.service.gov.uk/media/69ae77ddc78869bf8eb8a509/fraud-strategy-web.pdf (accessed 12 March 2026).*

7 *Payment Systems Regulator, Unmasking how fraudsters target UK consumers in the digital age (December 2024), analysis of APP scam trends and platforms used by fraudsters in the UK, https://www.psr.org.uk/publications/general/unmasking-how-fraudsters-target-uk-consumers-in-the-digital-age/ (accessed 5 February 2026).*

APP fraud starts with scam exposure on digital platforms

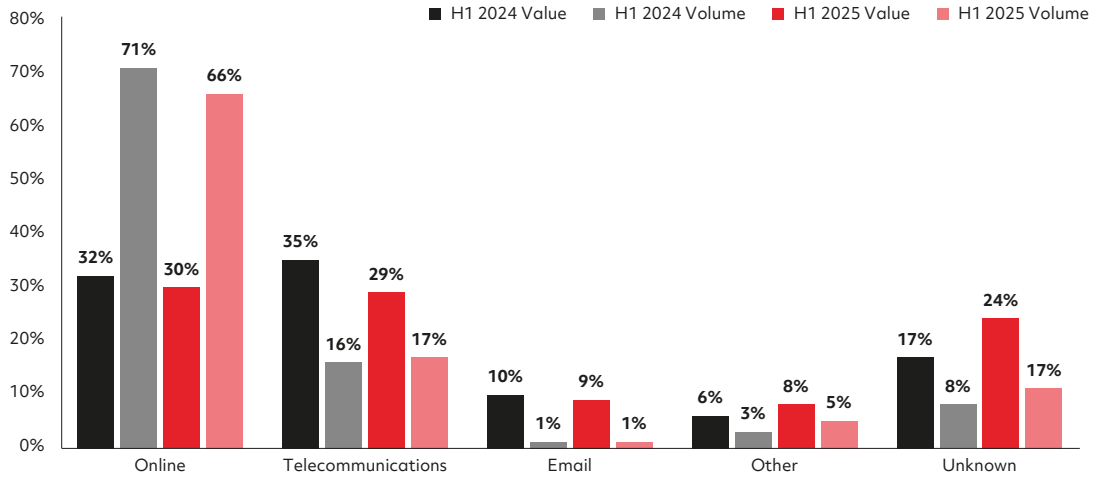
Today, a majority of authorised push payment (APP) fraud cases involve exposure to scams in online environments. As consumer activity has shifted online, organised criminal groups have followed. Social media platforms, online marketplaces, and messaging services now allow fraudsters to identify and contact potential victims at scale through targeted advertising, false identities, and algorithmic content amplification.



number of APP fraud cases originating in an online platform

Data from UK Finance for the first half of 2025 show that 66% of APP fraud cases in the UK are reported by victims as first encountered on online platforms, while 17% originate through telecommunications channels. Analysis from the Payment Systems Regulator (PSR) similarly indicates that most APP fraud begins online, with around 72% of cases linked to online platforms and up to 79% when digital communication channels such as messaging services and email are included.[8]

Where APP Fraud Cases Begin in the UK: H1 2024 vs H1 2025



The pattern is also reflected in government analysis. The UK Government's Fraud Strategy 2026–2029 notes that a substantial proportion of fraud now begins in online services, including social media platforms, messaging applications, and online marketplaces.[9]

8 *Payment Systems Regulator, APP scams data and analysis (including "Most common entities used by fraudsters … data covers 2023" and associated Meta share figures) https://www.psr.org.uk/authorised-push-payment-scams/scams-data/ (accessed 2 February 2026)*

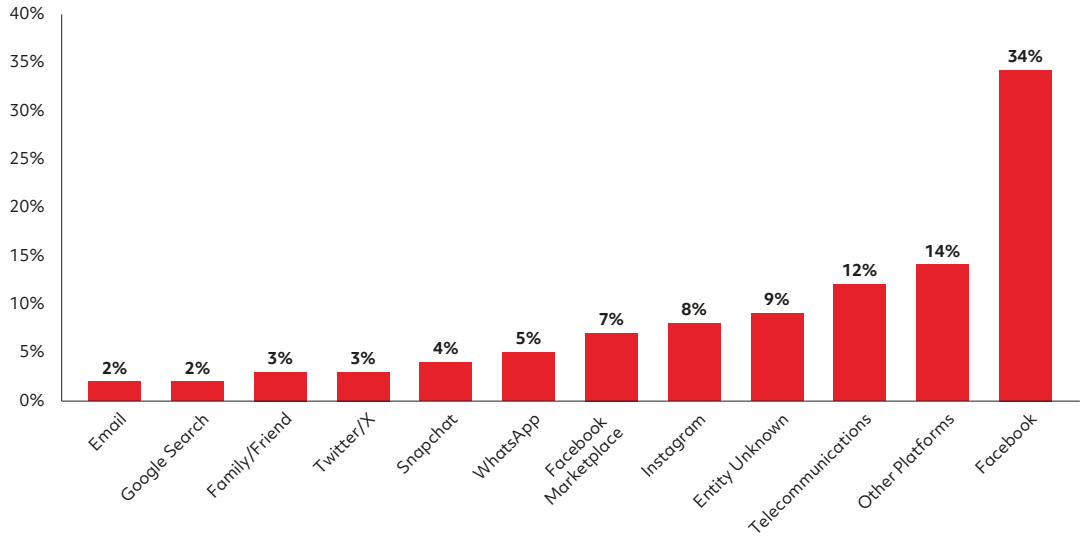
9 *Home Office, Fraud Strategy 2026–2029: Disrupting crime, supporting victims and building a safer, more resilient UK (March 2026), Chapter on "Drivers of the fraud threat" (online fraud origination and use of online services), https://assets.publishing.service.gov.uk/media/69ae77ddc78869bf8eb8a509/fraud-strategy-web.pdf (accessed 12 March 2026).*

The role of social media platforms in scam exposure

While scam exposure spans a range of digital environments, evidence from financial institutions consistently points to the central role of social media platforms. In particular, a small number of social media platforms repeatedly appear across datasets as sources of fraudulent content.

Most common entities used by fraudsters in the UK (by volume)

Data covers 2023



"A significant proportion of scams originate on the major social media platforms and their associated messaging ecosystems, where fraudsters are able to reach victims at scale."

Chris Ainsley
Head of Fraud Strategy

Santander

PSR data shows that £341 million was lost to APP fraud in 2023, with victims reporting Meta platforms as the originating platform in 54% of APP fraud cases and 18% of the total value of APP fraud. In other words, nearly £1 in every £5 lost to APP fraud in the dataset was linked to scams first encountered on Meta platforms.[10]

Evidence from individual financial institutions reinforces this concentration. TPA member Lloyds Banking Group found that two-thirds (68%) of purchase scams reported by its customers were first encountered on a Meta platform, principally Facebook and Instagram.[11] In its press release, it estimates that these scams alone cost UK consumers over £27 million annually, with victims often targeted through social media advertisements and digital marketplace listings. Based on its analysis of customer data combined with industry-wide estimates, **Lloyds Banking Group calculates that a consumer in the UK falls victim to a purchase scam originating on these platforms approximately every seven minutes.**

Multiple industry datasets support this trend. Revolut's Consumer Security and Financial Crime Report FY25 finds Meta-owned platforms were reported as the source of fraud for 44% of APP fraud cases globally.[12] The data reveals that Facebook accounts for over 21% of reported scam cases, while WhatsApp accounts for 17%, suggesting that both public social media feeds and private messaging services within the same platform facilitate scam activity.

10 *Payment Systems Regulator, Unmasking how fraudsters target UK consumers in the digital age (December 2024), analysis of APP scam trends and platforms used by fraudsters in the UK, https://www.psr.org.uk/publications/general/unmasking-how-fraudsters-target-uk-consumers-in-the-digital-age/ (accessed 5 February 2026).*

11 *Lloyds Banking Group, 'Two-thirds of all online shopping scams now start on Facebook and Instagram' (Press Release, 30 May 2023) https://www.lloydsbankinggroup.com/media/press-releases/2023/lloyds-banking-group-2023/two-thirds-of-all-online-shopping-scams-now-start-on-facebook-and-instagram.html (accessed 5 February 2026).*

12 *Revolut, Consumer Security and Financial Crime Report FY25 (PDF) https://assets.revolut.com/pdf/Revolut_Consumer_Security_and_FinCrime_Report_compressed.pdf (accessed 5 February 2026).*

"In many instances, the first interaction with a fraudster happens on the most popular social media platforms, whether through marketplace listings, adverts, or direct messages."

Laura Carter
Head of Fraud
Customer Experience

Santander

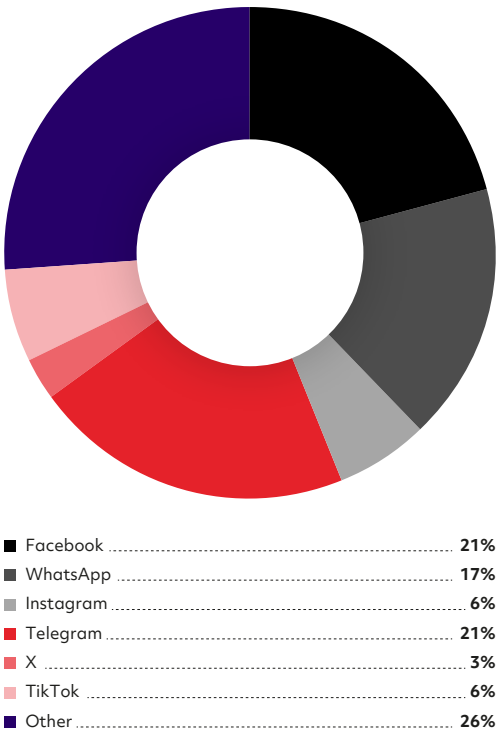
Messaging applications outside Meta's platforms are also emerging as prominent environments for scam activity. Telegram, for example, accounted for more than 20% of reported scam exposure in 2025.[13] These platforms allow fraudsters to communicate directly with victims, build trust, and carry out sustained social engineering.

TPA members interviewed for this research all identified social media platforms as common starting points for scams.

Farhana Hossain, Industry Engagement & Scams Strategic Change Enablement at Barclays, notes that many purchase scams begin on platforms such as Facebook Marketplace before victims are persuaded to make payments.

Rebecca Marriott, Chief Risk Officer at Tide, agrees. She describes social media platforms as a "huge driver" of scam exposure, particularly for purchase scams and romance scams, and like Hossain, she noted that these platforms frequently serve as the initial point of contact between fraudsters and victims, "after which interactions move into private communication channels where manipulation continues".

APP fraud by platform (2025)
% of total victims of APP fraud



Comments from Laura Carter, Head of Fraud Customer Experience at Santander UK, were also strikingly similar, noting that for many victims the first interaction with a fraudster "happens on the most popular social media platforms, whether through marketplace listings, adverts, or direct messages."

The multi-stage scam journey

APP fraud typically unfolds as a multi-stage process rather than a single event. Initial contact often starts on a digital platform, where victims encounter fraudulent advertisements, marketplace listings, or direct messages. Interactions then frequently move into private messaging environments, where fraudsters are able to build trust and carry out sustained manipulation before any payment is made.

Across member interviews, scams almost always follow a similar sequence:

1. Initial discovery and engagement through fraudulent advertisements, marketplace listings, or online posts
2. Migration into private messaging platforms, such as WhatsApp or Telegram
3. Exchange of payment instructions or bank details
4. Authorised transfer of funds by the victim

For victims, this is rarely a single deceptive message. It is often a sustained process of manipulation that can unfold over days or weeks before any payment is made.

13 *Revolut, Consumer Security and Financial Crime Report FY25 (PDF), UK platform distribution findings (Meta share, platform breakdown), https://assets.revolut.com/pdf/Revolut_Consumer_Security_and_FinCrime_Report_compressed.pdf (accessed 5 February 2026).*

How digital platforms facilitate scam activity

95bn

Scam ad impressions on social media in the UK in 2025

Digital platforms allow content, advertising, and messaging to reach large audiences quickly and efficiently. These same tools are routinely exploited by fraudsters to distribute scams at scale.

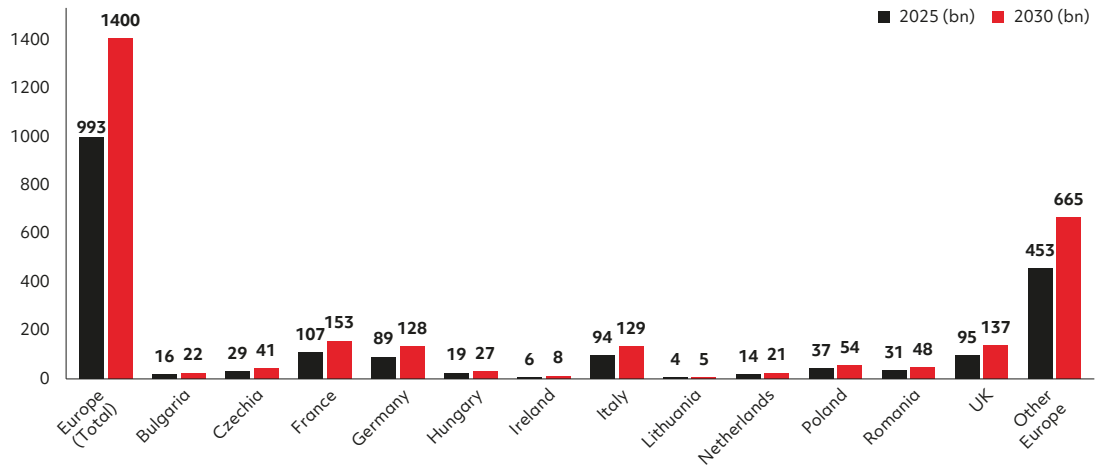
Fraudsters can create accounts, publish content, and engage with victims through both organic and paid channels. In many cases, they establish credibility and sustain engagement well before any financial transaction takes place.

Social media marketplaces now host large volumes of commercial activity, making it easier for fraudulent offers to appear alongside legitimate listings.

The scale of fraudulent advertising

Fraudulent advertising has become a major entry point for scams on social media platforms. These advertisements often impersonate brands, public figures, or investment services to attract victims.

Scam Ad Impressions on Social Media (bn)



Research highlights the scale of this activity across Europe and the UK. Juniper Research estimates that nearly one trillion scam advertising impressions (993 billion) were delivered to social media users in Europe in 2025, rising to 1.4 trillion by 2030.[14] In the UK alone, exposure is estimated at 95 billion scam advertisement impressions in 2025, increasing to 137 billion by 2030.

The scale of these impressions reflects how easily fraudulent advertisers can repeatedly deploy and replace scam promotions across large user bases. High advertising volumes increase the likelihood that users will encounter fraudulent promotions and engage with scammers.

Case study:

Investment scam originating on social media

In one widely reported UK case, a woman lost £75,000 after encountering a cryptocurrency investment advertisement on Facebook that falsely used the image of consumer advocate Martin Lewis.[15] After clicking the advert, the victim was directed to a fraudulent trading platform and persuaded to make an initial small investment.

Over time, scammers pressured the victim to transfer increasing amounts of money, ultimately extracting her life savings and additional loans.

The victim later stated that she had been "tricked, lied to and coerced" into transferring £75,000.

The scam began with a paid-for, but fraudulent social media advertisement and resulted in significant financial loss once payments were made. For victims, the consequences of these scams are rarely limited to financial loss. Many experience prolonged emotional distress and financial hardship long after the fraud has occurred.

Private messaging and migration

Private messaging services are widely used for legitimate communication, but they also allow scam interactions to move beyond publicly visible spaces.

As covered above, members of the TPA report that scams often begin through advertisements or marketplace listings before shifting into private messaging services such as WhatsApp or Telegram, where manipulation can continue over time, particularly in investment, impersonation, and romance scams.

Once interactions move into closed or encrypted messaging environments, scam activity becomes far less visible to both platform operators and financial institutions. This can make it significantly more difficult to identify suspicious behaviour before a payment takes place.

As a result, many fraud cases are reconstructed only after the event, often relying on screenshots or chat histories submitted by victims to understand how the scam unfolded.

14 *Juniper Research, Protecting Users from Scam Ads: A Call for Social Media Platform Accountability (white paper commissioned by Revolut, Feb 2026), scam ad impressions (Europe 993bn in 2025; Europe >1.4tr by 2030; UK 95bn in 2025 and 137bn in 2030) and scam-ad revenue charts (Europe £3.8bn; UK £430m in 2025), https://www.juniperresearch.com/resources/free-research/protecting-users-from-scam-ads-a-call-for-social-media-platform-accountability/ (accessed 15 March 2026).*

15 *The Guardian, 'Martin Lewis: I lost £75,000 due to Facebook scam adverts' (16 June 2023), victim account and context, https://www.theguardian.com/money/2023/jun/16/martin-lewis-lost-75000-facebook-scam-adverts (accessed 14 March 2026).*

Paid advertising and account creation

Paid advertising systems can amplify scam activity by placing content directly into users' feeds through algorithmic targeting. Sponsored content can appear especially credible when it resembles established brands or legitimate marketplace listings.

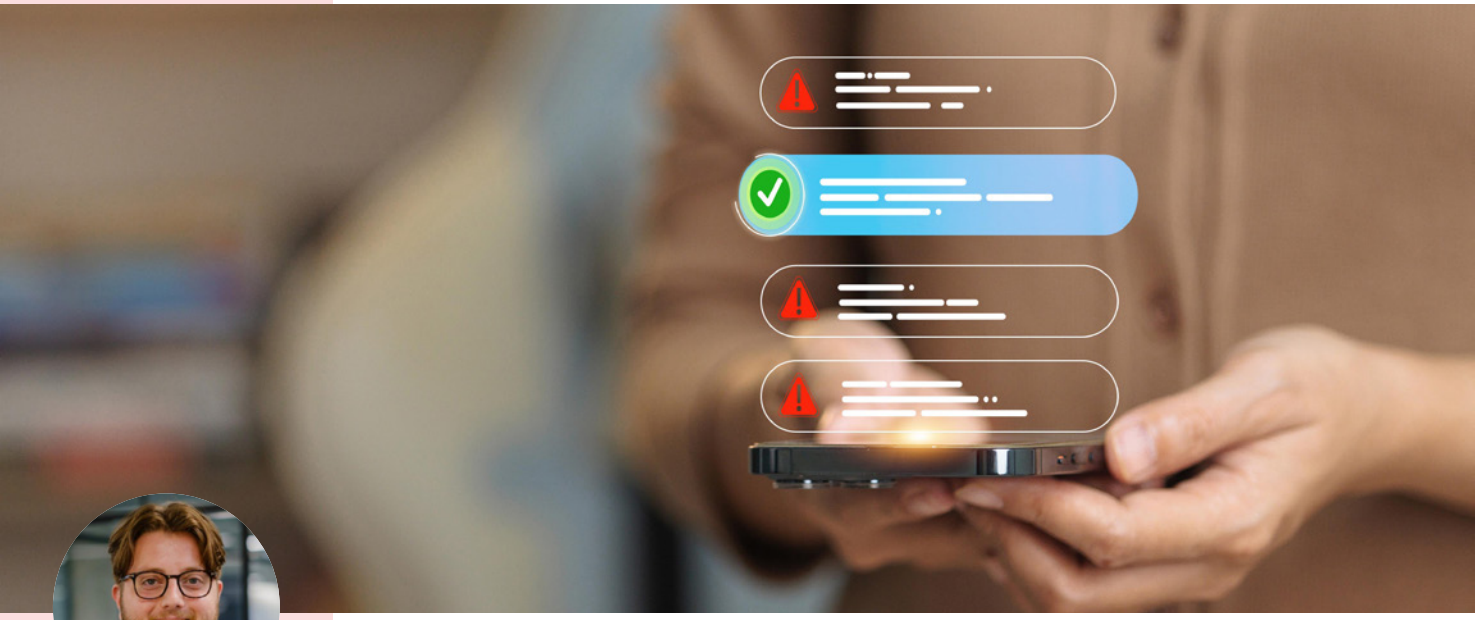
UK Government analysis highlights the role of digital advertising systems in enabling fraud at scale, noting that criminal actors frequently exploit online advertising networks to distribute fraudulent promotions and impersonation schemes.[16] However, key provisions under the Online Safety Act relating to fraudulent advertising are not expected to be fully in force until 2027, leaving a significant gap in the regulation of scam advertising.

Victoria Preece, Director of Compliance and Regulation at allpay, noted that targeted advertising systems can reinforce exposure to scam promotions: "You start searching for something online, and suddenly your social media feeds are filled with adverts for that item."

Access to these advertising systems depends in part on how advertiser accounts are created and verified. Account onboarding processes on many digital platforms are designed to provide rapid access for legitimate businesses, but they often involve limited identity verification. This can allow accounts to be created quickly, enabling advertising campaigns to be deployed at scale with relatively limited upfront scrutiny.

Where advertiser verification controls are weak, fraudsters can rapidly create new accounts and launch scam advertising campaigns before enforcement mechanisms detect and remove them. The strength of these controls varies across platforms and jurisdictions, with some platforms applying enhanced verification in higher-risk categories, while others maintain lower-friction onboarding processes. This raises serious questions about whether current advertiser onboarding and verification standards are adequate in higher-risk categories such as financial promotions or investment opportunities.

16 *UK Home Office, Fraud Strategy 2026–2029: Disrupting Crime, Supporting Economic Resilience and Delivering Justice (March 2026) https://www.gov.uk/government/publications/fraud-strategy-2026-to-2029 (accessed 16 March 2026).*



"We have flagged that an advert is fraudulent and requested it be taken down, and then we see the same advert appear again, or variations of it."

Rory Tanner
Head of UK Government Affairs

Revolut

Moderation and removal processes

Moderation systems often require a high level of certainty before content is removed, which can allow fraudulent advertisements to remain online for too long. Several TPA members reported cases in which scam advertisements remained online after being flagged or reappeared in modified forms after removal. These incidents were often associated with large social media advertising systems, such as those operated by Meta. They noted that scam campaigns operate through coordinated networks of accounts, allowing fraudulent content to be rapidly reposted or redistributed even after individual adverts are removed.

Investigative reporting has also highlighted weaknesses in platform advertising controls. In a Reuters investigation, a reporter was able to place fraudulent investment advertisements on Facebook and Instagram that were approved and distributed to thousands of users, despite clearly violating platform policies.[17] The ads were created with the assistance of intermediaries within Meta's own partner network, raising further questions about the effectiveness of advertiser vetting and oversight mechanisms.

Rory Tanner, Head of UK Government Affairs at Revolut, explained that he had seen instances in which fraudulent advertisements were detected and removal requests made, only for the fraudulent material to reappear or appear in different variations.

Dal Sahota, Global Director – Trusted Payments of LSEG Intelligence, notes that many scam campaigns operate through coordinated account networks, meaning "individual advert removals rarely stop the underlying activity".

This highlights the ongoing structural imbalance: while scam exposure occurs on digital platforms, responsibility for prevention and protection disproportionately falls with the payment system. The concentration of scam exposure within a relatively small number of platforms also suggests that prevention outcomes are influenced by platform-specific controls and enforcement approaches.

17 *Reuters, 'Meta's "trusted experts" helped me run scam ads on Facebook and Instagram' (15 December 2025), investigation into platform advertising controls, https://www.reuters.com/investigations/metas-trusted-experts-helped-me-run-scam-ads-facebook-instagram-2025-12-15/ (accessed 2 March 2026)*

The economics of the fraud chain

Digital platforms now play a central role in the distribution of scam advertising and fraudulent promotions. These platforms generate revenue whenever advertisers purchase placements within their advertising systems, regardless of whether the advertisements themselves are legitimate or fraudulent. As scam advertising has expanded across social media and digital marketplaces, it has also become a significant revenue stream within the wider digital advertising ecosystem.[18]

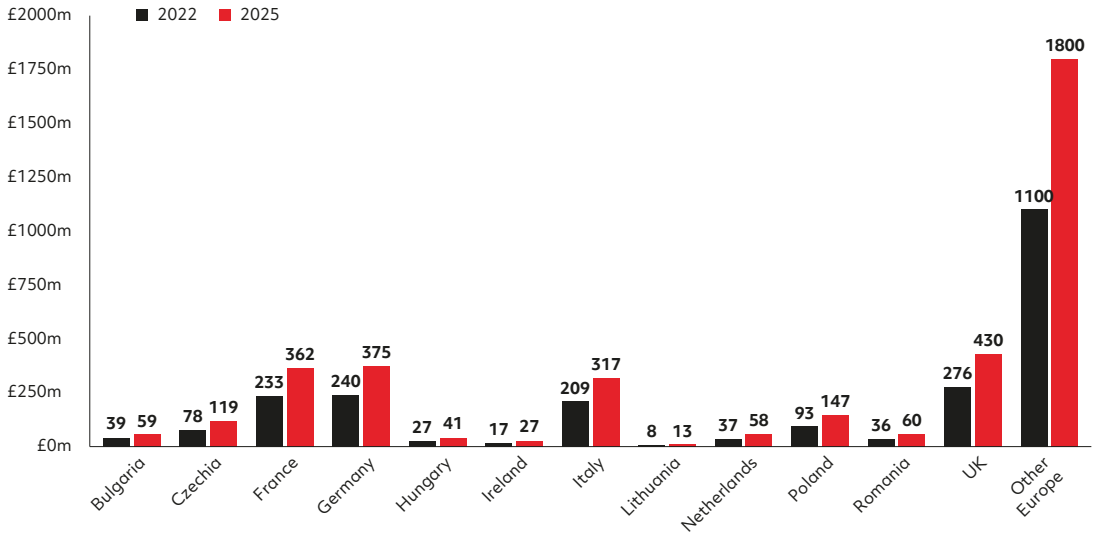
This dynamic creates a tension within digital advertising systems. Platform advertising models reward the distribution and amplification of content through paid promotion. When fraudulent advertisers access these systems, bad actors can generate significant advertising revenue for platforms while exposing users to potential fraud.

As explored in the previous chapter, estimates suggest that approximately 8% of social media advertisement impressions in the UK in 2025—representing around 95 billion impressions—are fraudulent. This figure is predicted to rise to 137 billion impressions by 2030 if no action is taken.[19] Across Europe, the equivalent figures are estimated at 10% (993 billion impressions) in 2025, with total impressions expected to reach 1.4 trillion across Europe in 2030.[20]

£430m

Social media revenue made from scam advertisements in the UK in 2025

Social Media Platform Revenue from Scam Ads (£m)



18 *The UK Government has acknowledged these risks within the Fraud Strategy, which notes that criminal actors are able to exploit digital advertising platforms to distribute fraudulent promotions and phishing campaigns at scale: UK Home Office, Fraud Strategy 2026–2029, Chapter 4.4 "Preventing the abuse of the UK's online infrastructure".*

19 *Juniper Research. 2026. Protecting Users from Scam Ads: A Call for Social Media Platform Accountability. White paper (commissioned by Revolut). Accessed February 10, 2026. https://www.juniperresearch.com/resources/free-research/protecting-users-from-scam-ads-a-call-for-social-media-platform-accountability/*

20 *Juniper Research. 2026. Protecting Users from Scam Ads: A Call for Social Media Platform Accountability. White paper (commissioned by Revolut). Accessed February 10, 2026. https://www.juniperresearch.com/resources/free-research/protecting-users-from-scam-ads-a-call-for-social-media-platform-accountability/*

Findings from Juniper Research show how lucrative these scam adverts can be, generating approximately £430 million in revenue for social media companies in the UK and £3.8 billion across Europe in 2025. These figures demonstrate that scam advertising represents a material revenue stream within digital advertising ecosystems.

Investigative reporting by Reuters similarly found that internal Meta documents projected that around 10% of the company's advertising revenue would derive from scam advertisements and other prohibited ads, while users may be exposed to billions of suspected scam ads each day.[21] Taken together, this evidence suggests that scam advertising is not a marginal issue within digital advertising systems, but a recurring and lucrative feature of large-scale platform advertising markets.

Revenue capture across the fraud chain

Scam advertising creates a misalignment between where revenue is generated and where financial harm occurs. When fraudulent advertisers purchase placements within digital advertising systems, platforms receive payment for distributing and amplifying those advertisements in the same way as legitimate campaigns.

Across the fraud chain:

- Platforms receive revenue when scam advertisements are distributed
- Fraudsters receive proceeds when victims transfer funds
- Financial losses typically emerge later within the payments system

This structure means that revenue from scam exposure can be captured before effective detection or intervention takes place, while the financial consequences materialise elsewhere in the system.

Platform system characteristics that enable scam exposure

Several structural features of modern digital platforms can inadvertently enable scam activity at scale.

- **Advertising infrastructure:** Self-service advertising systems allow rapid campaign deployment with limited upfront identity verification. Fraudulent advertisers can therefore create accounts and distribute scam promotions before moderation systems detect misconduct.
- **Algorithmic amplification:** Content recommendation systems prioritise engagement signals such as clicks and interaction rates. Scam advertisements often perform well under these metrics because they rely on urgency, financial incentives, or celebrity endorsements.
- **Account creation and re-entry:** Low-friction onboarding processes allow fraudsters to rapidly create replacement accounts after enforcement actions remove them. Without stronger identity verification or infrastructure fingerprinting, repeat offenders can quickly return.
- **Private messaging migration:** Public platform environments allow scammers to identify targets before moving interactions into encrypted or private messaging environments where moderation visibility is significantly reduced.

Together, these system characteristics can allow fraud campaigns to scale quickly before detection mechanisms typically intervene.

21 *Reuters, 'Meta created "playbook" to fend off pressure to crack down on scammers, documents show' (investigation, 31 December 2025), reported internal documents and allegations about operational responses to scam ads and revenue impacts, https://www.reuters.com/investigations/meta-created-playbook-fend-off-pressure-crack-down-scammers-documents-show-2025-12-31/ (accessed 5 February 2026).*

Where financial losses occur in the fraud chain

Financial liability for APP fraud in the UK currently rests primarily with payment service providers. Under the mandatory reimbursement regime introduced by the Payment Systems Regulator in October 2024, banks are required to compensate eligible victims of APP fraud when payments are executed through systems such as Faster Payments. Since these reforms came into force, a significant share of fraud losses has shifted onto financial institutions, even where the scam originated outside the banking system.

£173m

Amount of APP fraud reimbursed to victims between October 2024 - September 2025

Data from the Payment Systems Regulator's first year of monitoring indicates the scale of these reimbursement obligations. Between October 2024 and September 2025, around 88% of APP fraud losses (£173 million) were reimbursed to victims. This represents a significant increase compared with the 65% reimbursement rate reported by UK Finance in 2024, before the mandatory reimbursement regime was introduced. During the same period, consumers reported approximately 269,000 APP fraud claims, of which around 188,000 fell within the scope of the reimbursement requirement, and the majority were resolved within five business days. This represents a reduction of approximately 15% in reported claims compared with the previous year. While a significantly higher proportion of losses is now reimbursed to victims, these figures do not indicate that fraud is being reduced at source. Recent UK Finance data for the first half of 2025 also indicates that while some fraud types have declined, others—particularly unauthorised fraud—have increased, suggesting that fraud activity can shift between channels when controls are strengthened in one area.[22]

These reforms strengthened consumer protection at the point of payment, reducing the likelihood that victims would bear the financial consequences of scams. The 50/50 reimbursement split between sending and receiving firms was also a deliberate regulatory choice, intended to create shared incentives for both parties to prevent fraud. However, reimbursement obligations focus on the point at which the payment is executed rather than the earlier stages of the fraud lifecycle.

Alex Somervell, co-founder of Ask Silver, makes a similar point from a consumer-protection perspective. In APP fraud, banks often see the payment but not the underlying context, such as what the customer believes they are buying or why they are sending the money. "That gap makes it harder to distinguish an authorised scam payment from a legitimate transaction before the loss occurs."

Financial institutions typically detect scams only when a payment instruction is issued, by which point victims may already have encountered fraudulent advertising, interacted with scammers through messaging platforms, and undergone sustained manipulation. By this stage, victims may have already encountered fraudulent advertising, interacted with scammers on messaging platforms, and undergone sustained manipulation.

Rebecca Marriott, Chief Risk Officer at Tide, notes that banks frequently encounter scams only at the final stage of the fraud lifecycle: "By the time the payment reaches the bank, the customer has often already been exposed to the scam and manipulated elsewhere. At that point, we are trying to stop the outcome rather than the origin."

As a result, financial institutions are increasingly incurring direct financial losses from scams that originate elsewhere in the fraud chain. While digital platforms generate revenue from advertising exposure, the financial consequences of successful scams are typically absorbed downstream within the payments system or by consumers themselves.

This creates a clear policy challenge: the organisations responsible for reimbursing fraud losses are not always the ones that control the environments in which scams originate, and the platforms hosting the fraudulent content are actively profiting from this criminal activity.

22 *UK Finance, 'Half Year Fraud Report 2025', https://www.ukfinance.org.uk/system/files/2025-10/Half%20Year%20Fraud%20Report%202025_0.pdf (accessed 5 March 2026).*

Regulatory and international developments

Policymakers in several jurisdictions are increasingly recognising the role of digital platforms in enabling online fraud and are beginning to introduce regulatory frameworks to address it. Recent legislative and regulatory developments reflect a shift towards tackling fraud earlier in the fraud lifecycle, including in digital environments where many scams first arise.

In March 2026, the UK Government published its Fraud Strategy, setting out a system-wide approach to combating fraud across online platforms, telecommunications infrastructure, and financial services. The strategy emphasises disrupting fraud at source, strengthening intelligence sharing across sectors, and improving accountability for sectors that scammers exploit.[23]

These developments build on earlier reforms in the payments sector. In October 2024, the UK embarked on a significant reform of APP fraud by introducing mandatory reimbursement requirements. The framework has strengthened consumer protection at the point of payment, requiring PSPs to reimburse eligible victims of APP fraud, subject to defined exceptions. However, reimbursement obligations primarily focus on the execution stage of fraud rather than earlier exposure stages in the fraud lifecycle.

Together, these developments show regulators increasingly recognise that fraud prevention must extend beyond the point of payment into the digital environments where scam exposure occurs.

23 UK Home Office, Fraud Strategy 2026–2029: Disrupting crime, supporting economic resilience and delivering justice (March 2026).

"ECCTA lowers the threshold for attribution and shifts the focus from knowledge of wrongdoing to the adequacy of prevention."

Victoria Preece
Director of Compliance and Regulation

allpay

The Economic Crime and Corporate Transparency Act 2023

The UK's Economic Crime and Corporate Transparency Act (2023) ("ECCTA") aims to modernise the role of Companies House and enhance transparency across UK companies and other legal entities. Its purpose is to strengthen the business environment, support national security, and tackle economic crime, while providing a more reliable companies register to support legitimate business activity.

Importantly, ECCTA introduces a failure-to-prevent fraud offence applicable to large organisations operating in the UK.[24] Under this framework, liability could arise where:

- Fraud is committed for the benefit of the organisation; and
- Adequate prevention procedures were not in place

Victoria Preece, Director of Compliance and Regulation at allpay, notes that the legislation represents an important shift in how corporate responsibility for fraud may be interpreted. "The offence lowers the threshold for attribution and shifts the focus from knowledge of wrongdoing to the adequacy of prevention controls."

Although not strictly targeting scam advertising or messaging environments, ECCTA reinforces a broader regulatory principle: organisations may be expected to demonstrate effective prevention systems in areas under their operational control.

The Online Safety Act 2023

The UK's Online Safety Act (2023) marked an important turn in the governance of digital platforms and the mitigation of harmful or illegal content online. While the legislation was not specifically designed to address APP fraud, it imposes duties on certain online platforms to assess and mitigate risks associated with illegal content, including fraud facilitated by user-generated material and digital advertising. Provisions relating to user-generated content came into force in March 2025, while measures addressing fraudulent advertising are not expected to be fully implemented until 2027.

Under the Act, services designated by Ofcom as 'high-risk platforms' must implement proportionate systems and processes to prevent users from encountering fraudulent content. These obligations include measures on content moderation, reporting mechanisms, and enforcement procedures for removing illegal material. The Act also introduces duties on designated platforms to take reasonable steps to prevent users from encountering paid-for advertisements that promote scams or impersonation schemes.[25]

The UK Government's Fraud Strategy 2026–2029 reflects the weight of these provisions, stressing that systems enabling fraudulent advertising and online marketplace scams are significant drivers of modern fraud. It emphasises that online platforms, telecommunications providers, and financial institutions must work collaboratively to address vulnerabilities in the wider fraud chain, including those arising from digital advertising infrastructure.

While the Online Safety Act does not establish financial liability for fraud losses originating on digital platforms, it shows regulators now expect more from platforms. These developments reflect a growing recognition that digital platforms play a central role in where and how fraud begins.[26]

24 *Economic Crime and Corporate Transparency Act 2023, s 199 (failure to prevent fraud); and HM Government, 'Guidance to organisations on the offence of failure to prevent fraud' (10 October 2025), https://www.legislation.gov.uk/ukpga/2023/56/section/199 and https://www.gov.uk/government/publications/offence-of-failure-to-prevent-fraud-introduced-by-eccta/economic-crime-and-corporate-transparency-act-2023-guidance-to-organisations-on-the-offence-of-failure-to-prevent-fraud-accessible-version (accessed 5 February 2026).*
25 *Online Safety Act 2023; UK Home Office, Fraud Strategy 2026–2029 (2026), Chapter 4.4 "Preventing the abuse of the UK's online infrastructure".*
26 *Online Safety Act 2023, ss 38–41 (duties about fraudulent advertising; codes of practice), https://www.legislation.gov.uk/ukpga/2023/50/pdfs/ukpga_20230050_en.pdf (accessed 2 February 2026).*

European Union developments

In Europe, the Digital Services Act 2024 (DSA) introduces system-wide obligations for very large online platforms to assess and mitigate systemic risks associated with their services.[27] These risks include the spread of illegal content, such as online fraud and deceptive advertising.

Key requirements under the DSA include:

- Risk assessments
- Transparency reporting
- Independent audits
- Measures to mitigate identified harms

Together, these provisions require large digital platforms in the EU to take more proactive steps to reduce users' exposure to harmful or illegal content distributed through their services.

Alongside these platform governance reforms, the European Union is also strengthening fraud prevention within its payments framework. Recent developments within the EU payments legislative package, particularly the forthcoming Payment Services Regulation (PSR), include proposals to improve fraud in payment systems, including APP fraud, enhance information sharing between payment service providers, and introduce liability provisions that may involve multiple actors in the fraud chain when scams originate outside the payments system.[28]

At a policy level, the European Commission has also signalled plans to develop a broader EU strategy to combat online fraud.[29] This reflects growing recognition that many scams originate within digital platforms, advertising networks, and other online communication environments before reaching the payments system. Policymakers are emphasising preventive measures across the wider digital ecosystem, including stronger oversight of online advertising and closer cooperation between platforms, financial institutions, telecommunications providers, and law enforcement authorities.

Developments at the national level across EU member states also illustrate growing concern about the role of digital platforms in enabling online fraud. Across several EU member states, policymakers are increasingly examining the role of digital platforms. In France, for example, recent discussions around broader regulation of social media platforms have also prompted calls for stronger obligations on platforms to address scam advertising and other forms of fraudulent online promotion.[30]

Rory Tanner, Head of Government Affairs at Revolut, views the DSA as an important reference point for UK firms. He notes that formalised risk assessment and audit requirements for very large platforms provide a clearer accountability framework than voluntary commitments alone. In his view, where fraudulent content has been demonstrably flagged yet remains online, linking that failure to financial consequences "would bring about a material change".

27 *Regulation (EU) 2022/2065 (Digital Services Act), especially Articles on VLOP/VLOSE risk assessment, mitigation, audit and transparency reporting; EU text (English), https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng (accessed 2 February 2026).*

28 *European Commission, Proposal for a Regulation on payment services in the internal market, COM(2023) 367 final (28 June 2023), procedure 2023/0210(COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0367; and Council of the EU press release 'Payment services: Council and Parliament agree to step up the fight against fraud and increase transparency' (27 November 2025), https://www.consilium.europa.eu/en/press/press-releases/2025/11/27/payment-services-council-and-parliament-agree-to-step-up-the-fight-against-fraud-and-increase-transparency/ (accessed 2 March 2026).*

29 *A&O Shearman Financial Regulation blog, 'EC call for evidence on action plan for fighting online fraud' (26 January 2026), summarising the Commission call for evidence and scope, https://finreg.aoshearman.com/ec-call-for-evidence-on-action-plan-for-fighting-online-fraud (accessed 2 March 2026).*

30 *BBC News, 'France influencers: Jail threat for those found flouting new ad laws' (1 June 2023), legislation on influencer advertising and consumer protection, https://www.bbc.com/news/world-europe-65767265 (accessed 2 March 2026).*

Members interviewed for this research broadly regard the emerging EU approach as significant because it embeds prevention duties and supervisory scrutiny within the digital environments where scam exposure often begins. These developments point to growing recognition that effective fraud prevention requires coordinated responsibilities across platforms, payment institutions, and other actors across the fraud chain. Strengthening the analytical and technical capabilities of European law enforcement bodies to process complex fraud datasets is also frequently seen as an important element of this wider response.

International accountability models

While the UK's current framework concentrates liability primarily within the payments sector, various international jurisdictions are exploring alternative models that distribute responsibility more broadly across the wider fraud chain where scam exposure occurs.

These emerging frameworks emphasise a common principle: fraud often begins on digital platforms, including advertising and messaging environments. As a result, effective prevention requires coordinated responsibility across multiple sectors, rather than a sole focus on the point of payment.

Singapore: Attribution of responsibility across the scam chain

The Monetary Authority of Singapore (MAS) has implemented a Shared Responsibility Framework (SRF) to allocate financial responsibility for scam losses among different actors in the fraud chain.[31] Depending on where operational failures take place, this framework sees liability attributed to:

- Financial institutions
- Telecommunication providers
- And customers

As the framework has been implemented relatively recently, there is limited publicly available evidence on its long-term impact, though it provides a useful model for aligning incentives across the fraud chain.

The model is underlined by the principle that responsibility should follow the point of failure. For example:

- Banks may bear responsibility if adequate transaction warnings or intervention measures were not provided
- Telecommunications providers may be responsible where spoofed numbers or fraudulent messaging infrastructure were not sufficiently controlled
- Customers may bear responsibility where warnings were ignored

An accountability model like this creates incentives for each participant in the communication and payments chain. Consequently, prevention controls are strengthened within each area of influence.

While the Singapore framework's long-term impact is still being assessed, the model shows how responsibility for fraud losses can be distributed across multiple actors rather than concentrated solely at the point of payment. Notably, the framework currently focuses on financial institutions, telecommunications providers, and customers rather than digital platforms. However, it illustrates the broader policy principle that accountability can be aligned with those parts of the ecosystem where meaningful control over scam activity exists.

31 *Monetary Authority of Singapore and Infocomm Media Development Authority of Singapore, 'MAS and IMDA announce implementation of Shared Responsibility Framework from 16 December 2024' (media release, 24 October 2024); plus IMDA, 'Guidelines on Shared Responsibility Framework' (24 October 2024), https://www.mas.gov.sg/news/media-releases/2024/mas-and-imda-announce-implementation-of-shared-responsibility-framework-from-16-december-2024 and https://www.imda.gov.sg/-/media/imda/files/regulations-and-licensing/regulations/consultations/2024/shared-responsibility-framework-for-phishing-scams/guidelines-on-shared-responsibility-framework.pdf (accessed 10 March 2026).*

Australia: mandatory cross-sector intelligence sharing

Australia has taken a different approach, focusing on mandating intelligence sharing across the fraud chain.[32]

Through initiatives led by the Australian Competition and Consumer Commission (ACCC) and the National Anti-Scam Centre, authorities have developed cross-sector "fusion cell" models.[33] These models coordinate real-time intelligence between:

- Financial institutions
- Digital platforms
- Telecommunications providers
- Law enforcement

Participant organisations provide data on scam infrastructure, fraudulent advertising, and signals of mule account activity. For example, the National Anti-Scam Centre's "Fusion Cell" model enables banks, telecommunications providers, digital platforms, and law enforcement to share intelligence on emerging scam campaigns in real time and coordinate disruption actions, such as account takedowns, domain blocking, and payment interventions. Early evidence from the National Anti-Scam Centre indicates that this coordinated approach can deliver measurable disruption outcomes, including the removal of scam advertisements and websites and the prevention of victim contact, with initial pilots reporting reductions in certain scam categories, particularly investment scams.[34]

32 *Australia has also introduced measures targeting scam advertising, reflecting a broader regulatory approach to platform-enabled fraud. Reuters, 'Meta vowed to stop illegal financial ads in Britain. It failed 1,000 times in a week' (18 March 2026), reporting on comparative enforcement of scam advertising controls, https://www.reuters.com/sustainability/boards-policy-regulation/meta-vowed-stop-illegal-financial-ads-britain-it-failed-1000-times-week-2026-03-18/ (accessed 3 March 2026).*

33 *National Anti-Scam Centre, Romance Scam Fusion Cell Final Report (March 2026), overview of fusion cell model, outcomes and takedown metrics, https://www.nasc.gov.au/system/files/26-03-rpt-nasc-romance-fusion-cell-d03.pdf (accessed 10 March 2026).*

34 *National Anti-Scam Centre, 'National Anti-Scam Centre taskforce report highlights value of joint effort to tackle romance scams' (6 March 2026), report on coordinated efforts and impacts of romance scam prevention initiatives in Australia, https://www.scamwatch.gov.au/news-alerts/national-anti-scam-centre-taskforce-report-highlights-value-of-joint-effort-to-tackle-romance-scams (accessed 18 March 2026).*

Lessons for UK & EU fraud prevention frameworks

The international models illustrated two key principles that are influencing global fraud prevention approaches:

1. Responsibility can be distributed across the fraud chain in which scam exposure occurs, rather than focusing solely on the payments sector
2. Mandatory coordination mechanisms, especially intelligence sharing and prevention standards, can materially improve institutions' ability to detect and disrupt fraud earlier in the scam lifecycle

For policymakers, these developments provide useful case studies in evaluating how shared responsibility frameworks and cross-sector coordination mechanisms might evolve.

These regulatory developments reflect a growing recognition that responsibility for fraud prevention extends beyond payment providers. At the same time, they bring into focus a broader policy question: whether current accountability frameworks accurately reflect the source of scam exposure within the digital ecosystem.

Regulatory roadmap for platform-enabled fraud

To align fraud prevention incentives across the digital ecosystem, regulators may consider a phased regulatory approach.

Phase 1: Prevention standards
Regulators establish minimum requirements for digital platforms operating advertising, marketplace, or messaging services. These may include advertiser identity verification, repeat-offender detection, and scam-ad screening systems.

Phase 2: Transparency obligations
Large platforms may be required to publish regular transparency reports covering scam-advertisement volumes, removal timelines, advertiser verification outcomes, and repeat-offender activity.

Phase 3: Structured intelligence sharing
Regulators mandate participation in cross-sector intelligence-sharing frameworks that connect platforms, financial institutions, telecommunications providers, and law enforcement.

Phase 4: Proportionate enforcement
Where systemic prevention failures are identified, regulators are empowered to impose proportionate penalties or corrective measures to ensure compliance.

Such a framework could align prevention incentives across the fraud chain while maintaining proportional regulatory oversight.

Core principles for shared liability and accountability

The concept of shared accountability and liability is grounded in the principle that incentives influence behaviour. With clear definitions of responsibility and financial consequences, organisations tend to invest more in prevention, detection, and fraud management. Applying this principle suggests that accountability should align with wherever prevention controls can be implemented.

"Prevention becomes a force for good for the customer and industry when attached to financial liability."

Rebecca Marriott
Chief Risk Officer

tide

Aligning accountability with agency

Across interviews, TPA members consistently emphasised that responsibility for prevention should align with all the parts of the fraud chain where actors can exercise control.

Where organisations control advertising systems, user onboarding processes, messaging environments, or algorithmic content distribution, they can also detect and disrupt scam activity.

This perspective does not imply a blanket, strict-liability standard for digital platforms in every instance of fraudulent content. Rather, it reflects a broader view expressed by TPA members and industry more generally that accountability frameworks should identify where prevention capabilities exist and where intervention is realistically possible.

Several interviewees highlighted the potential value of a shared accountability and liability framework. In practice, this principle applies where actors exercise material control over:

- Advertising systems
- Account onboarding and verification
- Content amplification algorithms
- Messaging architecture

In such cases, it may be appropriate for organisations to bear proportionate responsibility for mitigating associated risks.[35]

35 *Policy developments recognise that prevention responsibilities may extend beyond financial institutions where other actors control the environments in which fraud exposure occurs.*

Four core principles emerge:

1

Prevention should be prioritised over reimbursement redistribution
Mandatory reimbursement has strengthened consumer protection at the point of payment. However, compensation alone does not reduce the proliferation of scam content if upstream exposure environments remain unchanged.

Several TPA members interviewed stressed that organisations tend to invest more in fraud prevention when financial or regulatory consequences are at stake. As Rebecca Mariott, Chief Risk Officer at Tide, says, reimbursement reforms have demonstrated that attaching financial consequences to fraud outcomes drives investment in prevention and detection controls.

A shared accountability framework should therefore strengthen incentives for earlier intervention where scam exposure occurs.

2

Proportionate liability triggered by clear failures
Interviewed TPA members consistently rejected blanket or automatic cost transfer mechanisms, favouring instead a graduated model that links accountability to identifiable operational failures.

This approach would see shared accountability activated when clear indicators demonstrate that reasonable prevention measures were not applied.

Examples could include situations where:
- A platform has been formally notified of fraudulent content and fails to act within defined timeframes
- Repeated advertised misconduct is tolerated despite prior enforcement action
- Systemic moderation failures are identified
- Required prevention standards are demonstrably not met.

3

Mandatory intelligence sharing
Fraud prevention depends on timely, actionable information. Interviewed TPA members emphasise that a credible shared liability framework must require mandatory participation in a structured cross-sector intelligence-sharing system. Voluntary information-sharing initiatives can be effective where participation is widespread. However, where key actors do not engage, fraud activity can migrate towards less controlled environments, undermining the effectiveness of existing efforts.

This reflects the policy direction of the UK Government's 'Fraud Strategy 2026-2029', which highlights the need for coordinated information exchange between financial institutions, telecommunications providers, online platforms, and law enforcement to disrupt upstream in the scam lifecycle.

Such an infrastructure could include:
- Standardised fraud signal reporting
- Mule account intelligence exchange
- Real-time notification pathways
- Clear legal frameworks for sharing fraud intelligence while complying with data protection laws

Benefits of structured intelligence sharing would mean scam indicators are detected within one part of the fraud chain and acted upon more rapidly across others.

4

Transparency and auditability
Since payment institutions operate within audited regulatory environments, several interviewed TPA members stressed the importance of parity in oversight.

As Farhana Hossain, Industry Engagement & Scams Strategic Change Enablement at Barclays, noted, banks are already subject to detailed supervisory expectations for fraud prevention, monitoring, and reporting. "Extending comparable transparency expectations to digital platforms would enable regulators and industry stakeholders to assess prevention performance more consistently across the fraud chain."

A shared accountability and liability framework may therefore be accompanied by transparency and audit requirements relating to:

- Advertiser verification standards
- Detection and moderation thresholds
- Reporting and removal performance
- Escalation and remediation processes

These mechanisms would allow regulators to determine whether prevention systems are effectively operating in practice.

Expected behavioural effects

TPA members believe that a carefully designed shared accountability and liability mechanism may incentivise:

- Stronger advertiser verification controls
- Faster content removal following credible notification
- Enhanced moderation thresholds
- Improved detection of repeat offenders
- Structured intelligence sharing with financial institutions

Together, these changes would direct prevention incentives towards the earlier stages of the fraud lifecycle.

Safeguards and proportionality

Interviewed TPA members underscore the importance of proportionality and competition safeguards. Michael Ketchion, Senior Financial Crime Operations Manager at Allica Bank, cautioned that liability rules must avoid disadvantaging smaller firms: "We would not want a regime that inadvertently entrenches only the largest firms who can absorb liability costs."

Accordingly, a proportionate framework includes:

- Clear thresholds for liability triggers
- Defined notification standards
- Appeal and dispute resolution mechanisms
- Differentiation between systemic failure and an isolated incident
- Consideration of firm size and capacity

This emphasis on proportionate regulation is consistent with the UK Government's *Fraud Strategy 2026–2029*, which highlights the importance of coordinated action across sectors while maintaining a competitive and innovative digital economy.

What shared accountability and liability is *not*

Such a framework does not mean:

- Automatic reimbursement transfers to digital platforms
- Strict platform liability for individual posts, advertisements, or messages
- Retrospective penalties to social media firms for historic cases
- An adversarial regulatory model between financial institutions and technology firms

The objective is instead to strengthen consumer protection and improve prevention wherever possible. A proportionate framework should align incentives, improve transparency, and encourage earlier intervention across the fraud lifecycle.

Operational model for shared liability

A shared accountability framework should operate through a defined attribution process linking liability to the point of failure in the fraud chain.

This approach avoids blanket liability while ensuring that organisations responsible for preventable failures bear proportionate responsibility. Under such a framework:

Stage 1: Scam exposure: Where fraudulent advertising, impersonation accounts, or marketplace listings are hosted on a digital platform and reasonable prevention systems were not applied, platforms may bear proportionate liability.

Stage 2: Victim manipulation: Where scams rely on telecommunications infrastructure, such as spoofed numbers or messaging services without adequate safeguards, telecommunications providers may bear proportionate liability.

Stage 3: Payment execution: Where payment service providers fail to apply required transaction monitoring, warning systems, or intervention controls, financial institutions may bear responsibility.

In practice, liability attribution would be determined through evidence of operational failures, such as:

- Failure to remove flagged fraudulent advertising within defined timeframes
- Repeated advertiser account creation following enforcement actions
- Failure to apply required transaction warnings or payment interventions
- Failure to implement mandatory prevention controls

This model aligns accountability with operational control while preserving strong consumer protection through reimbursement mechanisms.

A cross-industry action framework

TPA members argue that fraud prevention is not something that any one organisation can tackle in isolation. Reducing APP fraud at scale requires coordinated action across the organisations that influence scam exposure, communication, and payment execution. This section outlines practical measures that could strengthen protections across digital platforms, payment institutions, telecommunications providers, and regulators.

Actions for digital platforms

TPA members interviewed emphasise that large digital platforms already possess significant technical capability to detect and disrupt scams within their advertising platforms.

Investigative reporting by Reuters has shown that Meta platforms strengthened scam-advertising controls in markets such as Singapore, where regulation required it, but did not necessarily apply the same measures globally. In this context, interviewees highlighted several platform controls that could be strengthened:

1) **Advertiser verification controls**
   i. Enhanced identity verification for advertising in high-risk categories
   ii. Additional onboarding checks for financial promotions
   iii. Monitoring of repeat account creation following enforcement action

2) **Rapid removal protocols**
   i. Defined service-level expectations for removal after credible notification
   ii. Escalation pathways for repeated advertiser misconduct
   iii. Transparent reporting of removal timelines

3) **Repeat offender detection**
   i. Cross-account behavioural analysis
   ii. Device and infrastructure fingerprinting
   iii. Shared signals for persistent fraud actors

Rebecca Marriott, Chief Risk Officer at Tide, notes that without "robust" advertiser verification, known fraudsters can re-enter digital platforms under new identities, with ease, undermining enforcement efforts.

Victoria Preece, Director of Compliance and Regulation at allpay, stresses that scam advertising platforms are now highly sophisticated and that onboarding for high-risk financial promotions should involve proportionate friction comparable to requirements in regulated financial services.

Dal Sahota, Global Director – Trusted Payments of LSEG Intelligence, emphasises the importance of detecting behavioural patterns across campaigns, rather than relying on isolated post removals. In his view, "cross-account analysis, infrastructure fingerprinting, and systematic monitoring of repeat advertising behaviour" allow platforms to "identify coordinated activity earlier".

Intelligence sharing infrastructure

A consistent theme across member interviews is that fraud intelligence remains fragmented. Banks, fintechs, intelligence providers, and digital platforms each hold partial visibility of scam activity, but no single actor has a complete view of the fraud lifecycle.

The UK Fraud Strategy 2026–2029 similarly emphasises the need for stronger intelligence sharing across financial institutions, telecommunications providers, online platforms, and law enforcement, alongside improved national capabilities to aggregate and analyse fraud data.

Likewise, Dal Sahota, Global Director – Trusted Payments of LSEG Intelligence, emphasises that without structured signal-sharing between advertising ecosystems and financial institutions, early indicators of coordinated scam activity remain siloed.

Rebecca Marriott, Chief Risk Officer of Tide, notes that improved data sharing through mechanisms such as CIFAS, the UK's fraud intelligence database, and enhanced screening can materially strengthen prevention outcomes.

Farhana Hossain, Industry Engagement & Scams Strategic Change Enablement at Barclays, notes that "by the time a payment is made, banks often have little visibility of the earlier interaction between the victim and the scammer." Much of this intelligence sits with other actors in the ecosystem, such as advertising platforms or messaging services, and is not routinely shared with financial services in time to inform intervention.

Similarly, Michael Ketchion, Senior Financial Crime Operations Manager at Allica Bank, explains that earlier-stage evidence, such as messaging exchanges or advertisement links, typically only reaches banks when customers submit it during reimbursement claims. Without mechanisms to share these signals earlier between platforms and financial institutions, detection and disruption often occur after funds have already been transferred.

"By the time a payment is made, banks often have little visibility of the earlier interaction between the victim and scammer."

Farhana Hossain
Industry Engagement & Scams Strategic Change Enablement

BARCLAYS

However, today, cross-sector data flows remain inconsistent in format, latency, and governance clarity, allowing repeat offenders to migrate across platforms and accounts faster than signals can be consolidated.

Peter Griffin, co-founder of AVIEL Intelligence, argues that the most useful form of data sharing is actionable mule account intelligence captured during live scam interactions and passed rapidly to payment providers. In his view, intelligence only becomes most meaningful when it reaches institutions quickly enough to stop a scam payment before it is made, rather than simply recording the fraud after the event.

A more structured intelligence-sharing framework would not constitute an open-ended data pool, but a structured system governed by defined inputs, thresholds, and accountability. Core components could include:

- Standardised fraud signal reporting across platforms, payment service providers, and intelligence partners
- Real-time dissemination of mule account intelligence with defined response expectations
- Structured alert channels for upstream scam indicators, including fraudulent advertising campaigns, impersonation accounts, and coordinated scam infrastructure
- Audit trails and reporting mechanisms to evidence response times and remediation actions
- Governance frameworks aligned with existing data protection requirements, ensuring lawful and proportionate information sharing

From voluntary commitments to enforceable outcomes

Multiple voluntary initiatives have attempted to reduce online-enabled fraud through information sharing, cooperation, and platform-led controls. However, industry reporting and stakeholder testimony indicate that these measures have consistently failed to deliver a sustained, system-wide reduction in scam exposure within digital platforms or in resulting APP fraud losses.

Accordingly, stakeholders interviewed for this white paper stress the importance of moving beyond voluntary approaches towards clear, enforceable expectations for actors, including digital platforms and telecommunications providers. In practice, this means:

- Minimum standards for advertiser onboarding, verification, and repeat-offender controls in high-risk categories
- Defined removal and response timeframes following credible notifications
- Mandatory participation in a structured intelligence-sharing mechanism, with auditability
- Transparency reporting that allows regulators, industry, and the public to assess performance over time

Enforcement should be understood as a mechanism for driving prevention. Where standards are clear and performance is measurable, organisations face stronger incentives to detect and remove scam activity earlier in the fraud chain.

As Chris Ainsley, Head of Fraud Strategy at Santander UK, notes, liability frameworks can strengthen fraud prevention by prompting organisations to respond more quickly to emerging risks.

Action for regulators

The UK Fraud Strategy 2026–2029 recognises that fraud increasingly originates within online platforms, telecommunications networks, and digital advertising systems rather than solely within the financial sector. It emphasises the need to disrupt fraud at its source and improve coordination across platforms, telecommunications providers, and financial institutions.

This direction implies a stronger regulatory role in establishing clear prevention standards and oversight. Interviewed members consistently emphasise that meaningful fraud reduction will require clearer regulatory duties for upstream digital platforms. In practice, TPA argues this would involve the following policy measures:

1. **Establishing enforceable prevention standards for upstream platforms:** Regulators should define minimum prevention standards for digital platforms whose advertising, marketplace, or messaging services facilitate scam exposure.
2. **Introduce defined response timelines for fraudulent content:** Platforms should be required to respond within defined timeframes when credible financial institutions, regulators, or other recognised reporting bodies report fraudulent content.
3. **Require transparency reporting on scam-prevention performance:** Large platforms should publish detailed transparency reports covering scam-detection volumes, removal timelines, advertiser verification outcomes, and repeat-offender activity.
4. **Mandate cross-sector fraud intelligence sharing:** Platforms should be required to participate in structured intelligence-sharing frameworks alongside financial institutions, telecommunications providers, and law enforcement.
5. **Enable enforcement where systemic failures occur:** Regulators should have the authority to investigate and impose proportionate penalties where platforms repeatedly fail to implement effective prevention systems.

TPA members also emphasise the importance of clear enforcement rules. Chris Ainsley, Head of Fraud Strategy at Santander UK, argues that without a defined feedback loop between banks and platforms, liability debates remain theoretical. Just as card scheme rules established clear enforcement rules, regulators should clarify evidential thresholds for compliance across the scam chain.

Farhana Hossain, Industry Engagement & Scams Strategic Change Enablement at Barclays, similarly notes that while banks operate under detailed supervisory expectations, equivalent prevention standards for large digital platforms remain less prescriptive. Greater transparency around takedown timelines, advertiser vetting processes, and repeat-offender controls could therefore support a more proportionate assessment of accountability.

Members broadly support a regulatory framework that mandates data collaboration across the fraud chain, introduces enforceable prevention standards, and aligns incentives so that responsibility for fraud prevention sits where scam exposure occurs.

"To reduce fraud levels in the UK, we need enforcement action that incentivises platforms to improve fraud prevention."

Rory Tanner
Head of UK Government Affairs

Revolut

Conclusion: Aligning responsibility across the wider fraud system

APP fraud is not just a payments issue. As we've seen, most scams begin upstream—on digital platforms, marketplaces and messaging services—yet banks, payment providers and consumers are the ones to absorb the financial losses. This structural gap allows fraud to scale unchecked, while upstream actors face few enforceable obligations. These losses also represent a transfer of funds from the UK economy to organised criminal networks, diverting money from productive activity and enabling further investment in increasingly sophisticated fraud operations.

Recent policy developments already point towards a more comprehensive approach. The Online Safety Act 2023 and the Digital Services Act both reflect growing recognition that digital platforms have an important role in preventing fraudulent content and deceptive advertising. However, existing frameworks still do not fully reflect how APP fraud operates in practice.

The Payments Association is calling on the UK Government, EU policymakers, and regulators to introduce enforceable measures on scam advertising and platform accountability. This should include:

- coordinated regulatory action on advertiser verification
- faster removal of fraudulent content
- structured intelligence sharing
- clearer accountability and financial repercussions when platforms repeatedly fail to prevent scam exposure at source

Without action, scams will continue to scale through digital platforms while financial institutions and consumers bear the consequences.

APP fraud is a consumer protection challenge that requires responsibility and control to be aligned. Where platforms operate systems that enable large-scale scam exposure, they should also be expected to play a proportionate role in preventing it. **That is essential if fraud is to be reduced at scale.**

References

- A&O Shearman Financial Regulation blog, 'EC call for evidence on action plan for fighting online fraud' (26 January 2026), https://finreg.aoshearman.com/ec-call-for-evidence-on-action-plan-for-fighting-online-fraud
- BBC News, 'France influencers: Jail threat for those found flouting new ad laws' (1 June 2023), legislation on influencer advertising and consumer protection, https://www.bbc.com/news/world-europe-65767265
- Economic Crime and Corporate Transparency Act 2023, s 199; HM Government, 'Guidance to organisations on the offence of failure to prevent fraud' (10 October 2025), https://www.legislation.gov.uk/ukpga/2023/56/section/199 and https://www.gov.uk/government/publications/offence-of-failure-to-prevent-fraud-introduced-by-eccta/economic-crime-and-corporate-transparency-act-2023-guidance-to-organisations-• on-the-offence-of-failure-to-prevent-fraud-accessible-version
- European Banking Authority and European Central Bank, '2025 report on payment fraud' (December 2025), https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202512.en.pdf
- European Commission, Proposal for a Regulation on payment services in the internal market, COM(2023) 367 final (28 June 2023), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0367; Council of the European Union, 'Payment services: Council and Parliament agree to step up the fight against fraud and increase transparency' (27 November 2025), https://www.consilium.europa.eu/en/press/press-releases/2025/11/27/payment-services-council-and-parliament-agree-to-step-up-the-fight-against-fraud-and-increase-transparency/
- Home Office, Fraud Strategy 2026–2029: Disrupting crime, supporting victims and building a safer, more resilient UK (March 2026), https://assets.publishing.service.gov.uk/media/69ae77ddc78869bf8eb8a509/fraud-strategy-web.pdf
- Juniper Research, Protecting Users from Scam Ads: A Call for Social Media Platform Accountability (white paper, commissioned by Revolut, February 2026), https://www.juniperresearch.com/resources/free-research/protecting-users-from-scam-ads-a-call-for-social-media-platform-accountability/
- Lloyds Banking Group, 'Two-thirds of all online shopping scams now start on Facebook and Instagram' (press release, 30 May 2023), https://www.lloydsbankinggroup.com/media/press-releases/2023/lloyds-banking-group-2023/two-thirds-of-all-online-shopping-scams-now-start-on-facebook-and-instagram.html
- Monetary Authority of Singapore; Infocomm Media Development Authority, 'MAS and IMDA announce implementation of Shared Responsibility Framework from 16 December 2024' (24 October 2024); IMDA, 'Guidelines on Shared Responsibility Framework' (24 October 2024), https://www.mas.gov.sg/news/media-releases/2024/mas-and-imda-announce-implementation-of-shared-responsibility-framework-from-16-december-2024 and https://www.imda.gov.sg/-/media/imda/files/regulations-and-licensing/regulations/consultations/2024/shared-responsibility-framework-for-phishing-scams/guidelines-on-shared-responsibility-framework.pdf
- National Anti-Scam Centre, 'National Anti-Scam Centre taskforce report highlights value of joint effort to tackle romance scams' (6 March 2026), report on coordinated efforts and impacts of romance scam prevention initiatives in Australia, https://www.scamwatch.gov.au/news-alerts/national-anti-scam-centre-taskforce-report-highlights-value-of-joint-effort-to-tackle-romance-scams
- National Anti-Scam Centre, Romance Scam Fusion Cell Final Report (March 2026), https://www.nasc.gov.au/system/files/26-03-rpt-nasc-romance-fusion-cell-d03.pdf
- Online Safety Act 2023, ss 38–41, https://www.legislation.gov.uk/ukpga/2023/50/pdfs/ukpga_20230050_en.pdf
- Payment Systems Regulator, 'APP scams reimbursement' (policy), https://www.psr.org.uk/authorised-push-payment-scams/app-scams-reimbursement/
- Payment Systems Regulator, 'APP scams data and analysis', https://www.psr.org.uk/authorised-push-payment-scams/scams-data/
- Payment Systems Regulator, Unmasking how fraudsters target UK consumers in the digital age (December 2024), analysis of APP scam trends and platforms used by fraudsters in the UK, https://www.psr.org.uk/publications/general/unmasking-how-fraudsters-target-uk-consumers-in-the-digital-age
- Regulation (EU) 2022/2065 (Digital Services Act), https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
- Reuters, 'Meta's "trusted experts" helped me run scam ads on Facebook and Instagram' (15 December 2025), https://www.reuters.com/investigations/metas-trusted-experts-helped-me-run-scam-ads-facebook-instagram-2025-12-15/
- Reuters, 'Meta created "playbook" to fend off pressure to crack down on scammers, documents show' (31 December 2025), https://www.reuters.com/investigations/meta-created-playbook-fend-off-pressure-crack-down-scammers-documents-show-2025-12-31/
- Reuters, 'Meta vowed to stop illegal financial ads in Britain. It failed 1,000 times in a week' (18 March 2026) https://www.reuters.com/sustainability/boards-policy-regulation/meta-vowed-stop-illegal-financial-ads-britain-it-failed-1000-times-week-2026-03-18/
- Revolut, Consumer Security and Financial Crime Report FY25 (2025), https://assets.revolut.com/pdf/Revolut_Consumer_Security_and_FinCrime_Report_compressed.pdf
- The Guardian, 'Martin Lewis: I lost £75,000 due to Facebook scam adverts' (16 June 2023), https://www.theguardian.com/money/2023/jun/16/martin-lewis-lost-75000-facebook-scam-adverts
- UK Finance, Half Year Fraud Report 2025 (2025), https://www.ukfinance.org.uk/system/files/2025-10/Half%20Year%20Fraud%20Report%202025_0.pdf
- UK Finance, 'Fraud continues to pose a major threat with over £1 billion stolen in 2024' (press release, 28 May 2025), https://www.ukfinance.org.uk/news-and-insight/press-release/fraud-report-2025-press-release
- UK Finance, 'Over £600 million stolen by fraudsters in first half of 2025' (press release, 24 October 2025), https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps600-million-stolen-fraudsters-in-first-half-2025