Future Finance

TACKLING PAYMENT FRAUD AT SOURCE

Fairer Accountability Across the System

Future Finance Collaborative Challenge Programme

In partnership with FinTech West · Hosted at Triodos Bank, Bristol · June 2026



1. Executive Summary

Fraud is the most common crime in the UK. It accounts for 45% of all crime and claimed an estimated 4.15 million incidents in the year ending September 2025.[1] Reported fraud losses totalled £3.5 billion in the year to October 2025, with an average loss of £10,300 per report.[2] The vast majority has a payment dimension, relying on a victim making a payment, whilst often the scam originated elsewhere. In most cases victims first encounter a fraudulent advertisement, marketplace listing or message on a messaging platform, well before any payment reaches the banking system. Meta-owned platforms accounted for 44% of authorised push payment scams reported based on anonymised data from the Revolut platform in 2025, with Facebook the single largest source of authorised fraud at over 21% and WhatsApp a further 17%.[25] Organised crime groups routinely reinvest the proceeds of fraud to scale their operations and in some cases to fund other criminal enterprises; overseas scam compounds, which may house individuals who have been trafficked and forced to perpetrate fraud, are a direct link between payment fraud and modern slavery.[24] Beyond individual harm, the wider costs are significant. The economic and social cost of fraud in England and Wales reached at least £14.4 billion in 2023-2024[23] , with harm to victims extending well beyond financial loss and reports of 92% experiencing emotional or mental health symptoms, 57% a physical health symptom, and 63% a lasting behavioural change.[21]

The systems designed to prevent fraud remain fragmented. Financial services institutions absorb the cost of detection and reimbursement. Education about fraud risk is patchy and currently predominantly delivered at the point of payment and less evenly across the various touchpoints where an individual may encounter a potential scam. The ability to understand and track fraud patterns is hindered by the intelligence and data being held independently across banks, law enforcement, and the technology sector. It is rarely pooled effectively or in a timely manner which supports an individual in the moment that they are being targeted.

This report is the output of a three-session Collaborative Challenge Programme, run in partnership between Future Finance UK and FinTech West, hosted at Triodos Bank in Bristol in June 2026. It brought together practitioners from financial services, academia, law and policy to examine a single question: **how do we tackle payment fraud at source and across a scam journey rather than managing it after the fact?**

Across three structured sessions using the Double Diamond methodology, the group moved from problem framing through deep exploration to a set of practical recommendations. The methodology is designed to resist allowing groups to quickly move to solutions before the problem is fully understood. In this case, that rigorous approach produced a shift in framing within the group from a victim-centred analysis to a structural one, focused on the points in the system where intervention is both possible and not yet applied.

The recommendations in this report are sequenced to build on existing and announced government programmes, rather than to duplicate or compete with them.

1. **Establish measurable accountability for the online platforms, marketplaces and communications providers through which fraud originates.** Industry bodies should use the Online Advertising Taskforce and related government engagement to propose minimum expectations for proportionate identity verification, rapid removal and escalation of reported fraud, preservation of evidence, repeat-offender controls, transparent reporting of fraud-origin data and consideration of financial responsibility where reasonable controls have not been applied.

2. **Turn participation in the Online Crime Centre into an operational cross-sector intelligence-sharing protocol.** Banks, platforms, telecommunications providers, payment firms and law enforcement should agree what intelligence is shared, in what format, against what evidential threshold, defining response times and feedback requirements. Initial pilots should focus on a small number of types of fraud and measure fraudulent accounts, adverts and communications disrupted, payments prevented and repeat use of identified infrastructure.

3. **Developing a voluntary friction framework as a sector innovation project.** This would address the current absence of an industry standard for responding to trigger-moment vulnerability. The framework would set out data signals and customer consent mechanisms aligned to product design principles for firms offering opt-in enhanced protection during high-risk life periods or lower-authentication channels. This is best developed as a sector-led innovation opportunity, designed to complement rather than duplicate the Home Office's Financial Safeguarding Scheme from 2026.

4. **Championing and accelerating cross-bank fraud victim intelligence sharing** is achievable because the legal basis, infrastructure and structural precedent already exist: the Data (Use and Access) Act 2025 provides lawful basis, the UK Finance Vulnerable Victim Notification Scheme offers a working model being expanded to all police forces, and CIFAS maintains a shared database, though focused on perpetrators rather than victims. The specific gap is that fraud victim status isn't consistently flagged across institutions in real time. Industry bodies should engage the Home Office's Data Strategy to push for mandatory fraud victim flagging as distinct from CIFAS's perpetrator-focused framework.

5. **Engaging the Victims Charter process** is a direct opportunity to shape minimum post-fraud standards ahead of the Charter's 2027 publication, while its content is still being consulted on with victims, law enforcement, support organisations and industry. Industry bodies should submit positions advocating a consistent definition of repeat victimisation risk, minimum standards for the period immediately following a fraud incident including a structured "protection period" with enhanced friction, and adoption of "financial exploitation" as the sector's standard term for fraud victimisation. These positions already align with the direction the Home Office and NCA are moving, so sector endorsement would strengthen their inclusion.

6. **Industry bodies to formally advocate for fraud prevention to be named as an explicit strand within the Financial Inclusion Strategy's financial education programme.** The policy infrastructure exists, financial education is now becoming part of the curriculum in primary schools in England, and the Home Office has committed to embedding fraud education in schools and universities from 2026/27. The two strategies are not yet formally connected. The financial services sector, with its existing education programmes and practitioner expertise, can provide the knowledge and expertise to bridge that gap.

2. Central Hypothesis

The programme opened with a working hypothesis inviting the opportunity to consider how the UK financial ecosystem must shift from reactive reimbursement to proactive, upstream prevention, detecting and disrupting fraud before the point of payment.

- How might the UK financial services ecosystem, telecom providers, and law enforcement collaborate more effectively to detect and prevent payment fraud earlier in the scam journey?

Over three sessions, the initial framing was tested and refined, resulting in 2 adjustments to the original statement:

1. Upstream prevention requires a shared understanding of where fraud originates and not just where it is detected. In the majority of authorised push payment (APP) fraud cases, the initial point of contact with the victim occurs online, on social media, through online marketplaces, or via digital communications.[3] The financial services sector typically detects or flags to the individual the potential of fraud only at the payment stage, by which point any social engineering may have already succeeded. Effective upstream intervention requires the ecosystem to engage and flag the potential for fraud earlier in that chain, connecting to where fraud begins and educating individuals at multiple points across their journey.
2. Vulnerability to fraud is better understood as a trigger-moment condition and not just within fixed demographic characteristics. Since individuals can experience vulnerable moments at any age, for example following bereavement, job loss, the onset of financial pressure, or during a major life transition and with the increasing sophistication of tools that fraudsters are using, designing interventions around fixed categories based on demographics misses that trigger moments are not related just to demographics. The group's recommendations reflect a more contextual and dynamic model of risk.

Payment fraud is not primarily an individual failing. It is a structural one. The financial services sector, the platforms where fraud originates, and the agencies that hold intelligence all have both the capacity and the responsibility to act.

The greatest opportunity for the sector lies in strengthening the architecture that connects them and introducing prompts for individuals throughout the scam journey.

3. Scale of the Problem

The following data, drawn from published government and regulatory sources, framed the group's analysis throughout the programme.

45%	Fraud's share of all crime in the UK (year ending September 2025)[1]
4.15m	Fraud incidents against individuals (year ending September 2025)[1]
£3.5bn	Total reported fraud losses to Action Fraud (year ending October 2025)[2]
£629.3m	Stolen from financial services customers in the first half of 2025 alone[4]
88%	Of in-scope APP fraud losses reimbursed in the mandatory reimbursement scheme's first year (£173m)[4]
34%	Rise in investment scam losses in 2024, to £144.4m — average loss per victim is growing[5]
96%	Of 13-18 year olds transact online, 14% believe they have been defrauded[6]
770+	Under-18s convicted of money laundering in a five-year period; youngest aged 10 (University study, 2026)[7]

Two patterns are particularly significant for the sector's response.

- Fraud is shifting in profile. While total APP fraud cases fell 6% in the year to June 2025, investment scam losses rose sharply, suggesting fraud is migrating toward higher-value, harder-to-detect typologies that target more financially active individuals.[5] The sector's detection capabilities, calibrated to identify high-volume lower-value fraud, may be less effective against this evolving pattern.
- Young people are increasingly at risk. The most recent government data confirms that 96% of 13-18 year olds transact online and 14% believe they have experienced fraud.[6] Research published by the University of Bristol and Cardiff University in 2026, drawing on Freedom of Information requests to all UK police forces, found that more than 770 under-18s were convicted of money laundering offences over a five-year period.[7] The 18-24 age group has been identified by the Ministry of Justice as the cohort most susceptible to financial exploitation.

References

[1] Home Office, Crime Survey for England and Wales (CSEW), year ending September 2025, published in the UK Fraud Strategy 2026-2029.

[2] Action Fraud / Home Office, Report Fraud reported losses, year ending October 2025, published in the UK Fraud Strategy 2026-2029.

[3] UK Finance and Ofcom collaborative data, cited in the UK Fraud Strategy 2026-2029: 70% of APP cases start online.

[4] UK Finance, Half Year Fraud Report 2025, cited in the UK Fraud Strategy 2026-2029.

[5] UK Finance, Fraud Report 2025, cited in Future Finance programme materials, June 2026.

[6] Home Office, UK Fraud Strategy 2026-2029, para. 83, citing research on 13-18 year old online transactions.

[7] Ryder, N. et al. (2026), Money Mule Study: Arrests, Charges, Prosecutions and Convictions across UK Police Forces. Funded by Jockey Club Trust. Bristol/Cardiff Universities.

4. Three Structural Themes

Across all three sessions, three structural and interconnected themes recurred consistently.

4.1 The Gap Between Where Fraud Starts and Where the Sector Engages

Financial services fraud defences are concentrated at the payment stage, via increasing the tools and interventions to detect fraud, through increasing friction into the payment process, all in an attempt to reduce it. The responsibility is placed on the individual and the financial services organisation, after social engineering and the fraud initiation has taken place with over 70% of APP fraud cases now beginning online, in social media, online marketplaces, and digital communication channels, well before a payment instruction is made.[3]

This creates a structural gap. The financial services sector has limited visibility of the social engineering that precedes a payment, and limited formal connection to the platforms and communications providers through which it occurs, leaving it, as the Government's Fraud Strategy itself acknowledges, as the last line of defence in disrupting fraud that typically originates upstream.[26]

Closing this gap requires a response across the platforms and associated touchpoints, ensuring better intelligence sharing between the financial services sector and the upstream channels where fraud originates and a sector voice in the policy conversations that shape those channels' obligations.

The Government's newly established Online Crime Centre (OCC), launched in 2026 with £31 million of investment, is designed precisely to bring together partners from the financial, telecommunications, and technology sectors to share intelligence and develop coordinated responses.[8] The sector's active participation in the OCC, both as a data provider and as a co-designer of interventions, is the most direct route to closing this gap.

[8] Home Office, UK Fraud Strategy 2026-2029, paras. 32-39. The OCC is led by the Home Office and NCA, working with the City of London Police.

4.2 Vulnerability as a Trigger-Moment Condition

Vulnerability to fraud is frequently triggered by an external life event, bereavement, relationship breakdown, job loss, the cost-of-living pressure that intensifies in autumn and winter and at a key point in life, such as a transition to independent financial life at university. These are moments when an individual's normal decision-making processes are disrupted and when their susceptibility to social engineering increases.

This framing has practical implications for product design and customer journey. A vulnerable customer flag applied to a defined demographic group will miss the majority of people who are in a vulnerable moment at any given time. A model that uses behavioural signals to identify trigger-moment risk in real time is required to combat the sophisticated, constantly adapting fraud approaches and scams. Indicators such as changes in transaction patterns or contact channel shifts can be derived from open-banking.

The Financial Inclusion Strategy (November 2025) is relevant here. It explicitly recognises that vulnerability is contextual, not fixed, noting that 'consumers' circumstances change over time, they can move in and out of vulnerability'.[9] The FCA's Consumer Duty framework extends this logic into firms' product design obligations. The group's view is that the sector has the tools to operationalise this in fraud prevention, and should do so.

[9] HM Treasury, Financial Inclusion Strategy, November 2025, p.13.

[10] FCA, Consumer Duty, finalised guidance FG22/5, July 2022.

4.3 Intelligence Sharing: Legally Permitted, Institutional Collaboration Lacking

The Data (Use and Access) Act 2025 establishes fraud prevention as a lawful basis for sharing data across institutions [27]. A customer flagged as a fraud victim within one institution is not flagged across others, creating the conditions for repeat victimisation, a pattern well-documented in the research literature and in the group's discussions. Fraud victims are statistically more likely to be targeted again. As their data is frequently shared on criminal networks following the initial incident, the financial services industry should adopt a similar mindset to identify a solution for sharing this data, supporting the individual customer in addition to industry.

The Government's Fraud Strategy identifies this explicitly, noting that 'data fragmentation and sharing barriers' are one of the central obstacles to effective fraud prevention.[11] The OCC is intended in part to address this, facilitating organisations across the financial ecosystem to participate actively and consistently.

The group also noted that the Motor Insurers' Bureau offers a relevant structural precedent, an independent, not-for-profit intermediary funded by the industry as a whole, which removes competitive advantage as a barrier to collective action. An equivalent mechanism for fraud victim intelligence was proposed as a medium-term goal.

[11] Home Office, UK Fraud Strategy 2026-2029, Annex C, para. 4.

[27] Data (Use and Access) Act 2025 (c.18), amending UK GDPR Article 6(1)(ea) to introduce 'recognised legitimate interests' as a lawful basis for processing, including fraud prevention, fraud detection and crime prevention.

5. The Fraud Journey: Where the Sector Can Intervene

A key output of the programme was the mapping of the payment fraud journey from the fraudster's perspective, from initial contact through to payment and the identification of specific intervention points at each stage.

STAGE 1 — ORIGINATION: FIRST CONTACT AND SOCIAL ENGINEERING

What happens

The majority of fraud begins online. A fraudulent listing, a scam advertisement, or a social media approach creates the initial contact. The victim is drawn into the transaction, at times with limited ability to verify the validity of the seller and with a key focus on ease of engagement to facilitate the transaction.

What is the scale of the problem

Online channels are the dominant origination environment for fraud. Of all authorised push payment (APP) fraud cases, 70% begin online, through social media, online marketplaces, and digital communications, with 16% originating via telecoms channels. Those telecoms-originated cases account for 36% of total losses, reflecting the higher-value nature of voice-based social engineering.[3] The financial services sector typically encounters the fraud only at the payment stage, by which point the social engineering has already concluded.

The personal impact extends well beyond financial loss. A survey of fraud victims cited in the Fraud Strategy found that 92% experienced emotional or mental health symptoms following the fraud, 57% experienced a physical health symptom, with 63% reporting a behavioural change, including becoming more cautious about financial engagement, which itself reduces economic participation, impacting individual financial wellbeing.[21] These harms are not proportional to the amount lost. Significant psychological harm has been documented in cases involving relatively modest financial loss.

[3] UK Finance (2025), cited in Home Office, UK Fraud Strategy 2026-2029, Section 4.4. [21] Home Office, UK Fraud Strategy 2026-2029, para. 15. Citing: survey of fraud victims on emotional, physical and behavioural impact.

Where existing work is already underway

- The Online Advertising Taskforce, co-led by DCMS and the Home Office, is developing industry recommendations on the obligations of online platforms in relation to fraudulent advertising, with a report due by Q1 2027.[14]
- The OCC will share intelligence with digital and technology sector partners to enable them to improve their trust and safety capabilities.[8]
- The Stop! Think Fraud campaign, expanded from 2026, aims to build public resilience across a broader range of fraud types.[13]

Where the sector can focus

Coordinated, evidence-based intelligence from the financial services sector about the origin channels of fraud, which platforms, which typologies, which time periods, is a direct input into both the OCC and the Online Advertising Taskforce's work. Structured contribution of anonymised, aggregated origin intelligence is an area of meaningful sector influence to demonstrate the scale of the issue and has the largest opportunity to improve the consumer journey.

[13] Home Office, UK Fraud Strategy 2026-2029, para. 5.

[14] Home Office, UK Fraud Strategy 2026-2029, Annex A Delivery Plan.

STAGE 2 — PAYMENT: TRANSACTION PROCESSING AND FRICTION

What happens

The payment stage is where the sector's defences are currently strongest with confirmation of payee, reimbursement obligations, and behavioural analytics all operating here. The group identified two specific gaps.

- Friends and family payment designation is actively exploited by fraudsters to bypass fraud checks, on the basis that such payments are treated as lower risk.
- Although APP fraud reimbursement is a significant consumer protection it does not prevent the harm, it rather responds to it neglecting the benefit of response earlier in the process to positively impact an individual's financial health. Whilst the sector's investment in detection capability at the payment stage is valuable, the reimbursement framework creates a risk that individuals treat reimbursement as a substitute for prevention.

What is the scale of the problem

- At least £629.3 million was stolen from financial services customers in the first half of 2025 alone, the majority through unauthorised fraud types (£371.8 million), with bank and credit account fraud rising 19% to 2.6 million cases in the year ending September 2025. (4)
- APP fraud reimbursement, while important, does not resolve the harm. In its first year of mandatory operation (from October 2024), 88% of in-scope losses were reimbursed, representing £173 million returned to victims. (4) This figure captures only in-scope, reported APP fraud. Investment scam losses rose 34% in 2024 to £144.4 million, with average losses per victim growing, indicating that fraud is migrating toward higher-value, harder-to-detect typologies that fall partially outside current reimbursement coverage. (5)
- The financial and emotional consequences are compounding with 92% of fraud victims reporting emotional or mental health symptoms; 57% a physical health impact; and 63% a change in financial behaviour. (21) A reimbursement framework does not address these downstream effects.

Where existing work is already underway

- The PSR is keeping the mandatory reimbursement scheme under review. The Home Office will launch a Call for Evidence on unauthorised fraud in Q4 2026.[15]
- Mandatory APP fraud reimbursement within the Faster Payment System has been in place since October 2024. In its first year, 88% of in-scope losses were reimbursed.[4]
- Confirmation of Payee (CoP) is in operation, though the group noted it is regularly worked around by fraudsters who instruct victims to confirm incorrect details.

Where the sector can focus

The group identified the concept of voluntary friction as an area for sector innovation, introducing a framework that allows individuals to opt into enhanced transaction checking during periods of known vulnerability such as major life events, significant account pattern changes, or self-declared high-risk periods. This is distinct from mandatory friction, which affects all customers regardless of risk, and from paternalistic profiling, which applies protective measures without the customer's knowledge.

A 'payment awareness score', an open banking-derived indicator of transaction literacy coupled with behavioural consistency, similar in concept to a credit score, was proposed as a tool that could inform both voluntary friction design and broader financial capability signposting. This is an area where fintech innovation and sector collaboration could produce a deployable product.

[15] Home Office, UK Fraud Strategy 2026-2029, Annex A Delivery Plan.
[16] PSR, APP Fraud Reimbursement: Mandatory Reimbursement, October 2024.

STAGE 3 — MULE ACCOUNTS AND MONEY MOVEMENT

What happens

Once a payment is made, proceeds move rapidly through the system via money mule accounts, often held by young people who may not fully understand their involvement in a criminal enterprise, and are then layered through multiple transactions to obscure origin.

The 2026 University of Bristol and Cardiff University money mule study, using Freedom of Information data from all UK police forces, found that the 18-24 age group is the most susceptible to involvement in exploitative money laundering.[7]

What is the scale of the problem

- Money muling operates at a significant scale and disproportionately draws in young people, often without their understanding of the criminal nature of their involvement. Research published by the University of Bristol and Cardiff University in 2026 drawing on Freedom of Information data from all UK police forces found that more than 770 under-18s were convicted of money laundering offences over a five-year period, the youngest aged ten.[(7)]

Home Office-commissioned research by Ipsos UK, published July 2026, provides the first detailed picture of lived experience. Key findings directly relevant to the sector's response are:[(22)]

- 53% of survey respondents had either never heard of the term 'money muling' or did not know what it meant, confirming that awareness, not complicity, is the primary entry risk for many individuals.
- 80% of money muling activities reported in the survey were carried out at the request of someone known to the individual, a friend, romantic partner, or family member, rather than a stranger.
- 60% of those who engaged in money muling had previously been fraud victims whilst 37% had experienced another crime in the previous five years, establishing a direct statistical link between prior fraud victimisation and subsequent exploitation as a mule.
- Financial instability was the most common life circumstance linked to involvement: 51% had experienced severe financial stress, 41% had lost their job in the last five years.
- Education about consequences is more effective when framed in tangible, personal terms: loss of access to a mortgage, student loan, or phone contract was found to be more resonant with young people than the abstract threat of criminal prosecution.

These findings have direct implications for both the sector's customer communications and for the financial education content it supports. They also confirm the case for a structured cross-bank victim flagging mechanism where a person identified as a fraud victim by one institution is, statistically, at elevated risk of exploitation as a money mule and that risk is not currently flagged across institutions.

[22] Home Office / Ipsos UK (2026). Lived Experiences of Money Muling. Published 16 July 2026. Available: https://www.gov.uk/government/publications/lived-experiences-of-money-muling/lived-experiences-of-money-muling

Where existing work is already underway

- The FCA is analysing 'cashing-out' methods and will share findings with industry, while identifying barriers to tackling exploitative money laundering.[17]
- The NCA's money mule working group brings together financial services and technology firms. Ipsos research commissioned by the Home Office on money muling pathways, showing how individuals become involved and how they exit. [22]

- The Home Office is working with The Children's Society to establish referral pathways for children and young people identified as victims of financial exploitation related to exploitative money laundering.[17]
- A dedicated Fraud PREVENT lead within the City of London Police will coordinate targeted education and interventions for individuals at risk from 2026.[17]

Where the sector can focus

A cross-bank fraud victim flagging mechanism, sharing data on individuals identified as fraud victims to prevent repeat victimisation and to flag associated mule account activity, is a structural intervention available where the legal basis already exists under the Data (Use and Access) Act 2025 [27]. This requires institutional collaboration both within the sector and across the journey.

UK Finance's Vulnerable Victim Notification Scheme, which allows law enforcement to flag concerns about an individual's financial vulnerability to the financial services sector, is a model that the Government has committed to expanding to all police forces.[18] The sector's role is to ensure that this expansion is treated as a priority, build the business case where required for additional funding and the scheme's architecture supports effective, real-time flagging.

[17] Home Office, UK Fraud Strategy 2026-2029, paras. 94-97.

[18] Home Office, UK Fraud Strategy 2026-2029, para. 92.

STAGE 4 — IMPACT AND REPEAT VICTIMISATION

What happens

Fraud victims face harm beyond financial loss, research documents significant psychological and emotional impact, including shame, self-blame, all reducing confidence in financial services. Fraud victims are at statistically elevated risk of being targeted again with data frequently resold through criminal networks.

What is the scale of the problem

- The impact of fraud on victims extends well beyond the immediate financial loss and is frequently underestimated in institutional responses. A survey of fraud victims cited in the Fraud Strategy found that 92% experienced emotional or mental health symptoms following the incident, 57% experienced a physical health symptom whilst 63% reported a lasting behavioural change.(21) The Home Office notes that psychological harm does not always correlate with the amount of money lost, suggesting that low-value fraud can cause significant long-term harm.
- Repeat victimisation is both statistically significant and structurally enabled by current intelligence practices. Fraud victims' data is frequently resold on criminal networks following the initial incident, increasing the likelihood for retargeting, elevating individuals' vulnerability. The Ipsos money muling study found that 60% of individuals who became money mules had previously been fraud victims.(22)
- The long-term economic consequences compound over time.This may include reduced confidence and engagement in financial services and potentially loss of access to banking, mortgages, phone contracts, and employment, where money muling is involved.

Where existing work is already underway

- The Home Office will introduce a Fraud Victims Charter in 2027, setting national standards for the level of service every victim should receive, including response times, minimum standards of care, and clear communication pathways.[19]
- Report Fraud, the new streamlined reporting service, will provide bespoke protection advice to victims following report submission and feed intelligence into the National Intelligence Model.[19]
- The Financial Safeguarding Scheme, to be launched from 2026, will establish a more consistent approach to identifying individuals at financial risk and providing tailored safeguards before fraud or revictimisation occurs.[18]

Where the sector can focus

The language and framing used when a fraud victim is identified matters. The group recommends adopting 'financial exploitation' and 'person in a vulnerable moment' as standard institutional language, consistent with the direction the Home Office and NCA are already moving in. The aim of a shift in language is to change how firms respond, how customers are treated, and how data is categorised for intelligence purposes.

Firms can also use the Victims Charter consultation process, ahead of the 2027 implementation deadline, to advocate for specific minimum standards that reflect the sector's understanding of repeat victimisation risk and what effective post-fraud support looks like.

[19] Home Office, UK Fraud Strategy 2026-2029, paras. 103-104.

6. Six Actions for Industry Bodies

The following recommendations are addressed specifically to financial services industry bodies as organisations with the standing, networks, and convening power to take them forward. They are sequenced by immediacy.

1

Establish measurable accountability for platforms, marketplaces and communications providers

Fraud prevention responsibilities should reflect where fraud originates. Online platforms, marketplaces and communications providers should be subject to measurable expectations proportionate to the risk created through their services, rather than financial institutions carrying most of the operational and financial burden after a payment is made.

Industry bodies should develop a policy proposal for the Online Advertising Taskforce, government and regulators covering proportionate identity verification for advertisers and commercial sellers, implement rapid removal of reported fraudulent accounts whilst preserving evidence, introducing effective repeat-offender controls and standardised reporting of fraud origin, losses and outcomes.

Government should also examine proportionate financial incentives where persistent control failures materially enable fraud. Options for consideration could include contributions to prevention or victim-support activity, regulatory penalties or defined cost sharing. The recommendation is to test the principle and evidence, rather than to prescribe a single liability model at this stage.

2

Lead active participation in the Online Crime Centre

The OCC is designed to be the central intelligence-sharing and coordination mechanism for fraud prevention, bringing together the financial services sector, telecommunications, technology, and law enforcement. Industry bodies should ensure their members are active contributors, not passive observers: providing structured, anonymised data on fraud origin channels; co-designing detection protocols, utilising the OCC's intelligence outputs to update sector-wide guidance. Announced in March 2026 as part of the Fraud Strategy, the OCC began operations in April 2026, its effectiveness will depend directly on the quality and consistency of industry data contribution.

3

Develop a voluntary friction framework as a sector innovation project

There is no current industry standard for how firms should respond to trigger-moment vulnerability in a fraud prevention context. A voluntary friction framework, setting out the data signals, customer consent mechanisms aligned to product design principles that firms should apply when offering opt-in enhanced protection during high-risk life periods, or through channels where there is less protection and authentication. This approach would fill this gap, an industry innovation welcomed by consumers who are recognising the increasing sophistication of fraud, with those that would opt into additional friction to protect themselves. The ongoing work by banks to secure apps on

phones when stolen is an indication that banks and communication platforms are looking to reduce the number of incidents of fraud.

This is a sector-led innovation opportunity, appropriate for development through Innovate Finance's innovation workstreams or the Payments Association's industry engagement programmes. The framework should be designed to complement, not duplicate, the Financial Safeguarding Scheme being developed by the Home Office from 2026.

4

Champion and accelerate cross-bank fraud victim intelligence sharing

The Data (Use and Access) Act 2025 provides the lawful basis for cross-institution fraud victim data sharing. The UK Finance Vulnerable Victim Notification Scheme, which allows law enforcement to flag an individual's financial vulnerability to the sector, is an existing working model the Government has already committed to expanding to all police forces.[18] CIFAS, the UK's fraud prevention service, maintains a shared fraud database across member organisations. The infrastructure, the legal authority, and the structural precedent all exist. What does not yet exist is a consistent, sector-wide standard for how fraud victim status is flagged across institutions in real time, as distinct from fraud perpetrator flagging, which CIFAS's existing databases address.

The specific gap to address is where a customer identified as a fraud victim by one institution is not flagged to others, even though the Ipsos money muling research confirms that 60% of those drawn into money muling had previously been a fraud victim.[22] That elevated risk is invisible across the system.

Industry bodies should pursue two specific actions. First, engage with the Home Office's Data Strategy, the output of the closed economic crime information sharing call for evidence, to advocate explicitly for fraud victim flagging to be treated as a mandatory component of the cross-institution data sharing standard, separate from the existing CIFAS perpetrator-focused framework. Second, commission a scoping study, appropriate for Innovate Finance or UK Finance to lead, examining what a fraud victim flagging mechanism would require in practice: governance model, data standards, consent architecture, and relationship to existing CIFAS infrastructure.

On AI-assisted detection: firms across the sector are already exploring privacy-preserving approaches to shared fraud detection, including the use of synthetic transaction data to train detection models without exposing real customer data. This is a legitimate, developing area of fintech innovation. Development should be monitored to identify opportunities to champion and accelerate intelligence sharing.

5

Engage the Victims Charter process to establish minimum post-fraud standards

The Fraud Victims Charter is due in 2027. Its content is still being developed, in consultation with victims, law enforcement, support organisations, and industry. This is a direct engagement opportunity. Industry bodies should submit to the Charter's consultation process advocating for: a consistent definition of repeat victimisation risk; minimum standards for the period immediately following a fraud incident, including a structured 'protection period' during which enhanced friction is applied, in addition to the adoption of 'financial exploitation' as the sector's standard term for fraud victimisation. These positions align with the direction the Home Office and NCA are already moving, sector endorsement will strengthen their inclusion in the Charter.

6

Embed fraud prevention as a named strand within the Financial Inclusion Strategy's education programme

The Financial Inclusion Strategy (November 2025) commits to making financial education compulsory in primary schools in England for the first time, establishing the Money and Pensions Service's Money Guiders programme in healthcare and job centre settings, funding programmes to support financially excluded consumers to build financial skills and confidence.[20] Separately, the Fraud Strategy commits to embedding fraud and exploitative money laundering resources in schools from the 2026/27 academic year, developed in partnership with SWROCU and the PSHE Association, and to supporting university students' resilience to fraud through the Fraud PROTECT Network from 2026.[6]

These two commitments are complementary and should be formally connected. The Financial Inclusion Strategy contains no explicit reference to fraud as a component of financial capability, a significant gap, given that the same life circumstances that create financial exclusion (unemployment, financial instability, isolation) are the leading vulnerability factors for fraud victimisation, as the Ipsos money muling study confirms.[22]

The definition of financial capability directly encompasses what fraud victims lose: the knowledge, skills and confidence to manage money effectively. Fraud does not merely cause financial loss, it erodes the financial confidence and behaviours that financial education seeks to build. Addressing fraud within financial capability programmes therefore reinforces both agendas simultaneously.

Industry bodies are well placed to close this gap in three specific ways:

(1) formally advocating, through DfE and HM Treasury engagement channels, for fraud prevention to be named as a strand within the Financial Inclusion Strategy's financial education pillar.

(2) contributing sector-funded practitioner expertise and case study content to the SWROCU/PSHE school rollout and the university PROTECT Network programme.

(3) continuing to promote and support evidence based recommendations including but not limited to:

- the University of Bristol and Cardiff University fraud prevention curriculum, developed with educational psychologists, available free to English universities from the 2026/27 academic year, as a ready-made, evidence-based resource.

- the Ipsos money muling research provides specific guidance on content design: education that focuses on tangible personal consequences (inability to obtain a mortgage, student loan, or phone contract) is significantly more effective than abstract criminal prosecution framing, particularly with young people.[22] Lived experience stories demonstrating how trusted relationships can be exploited are more persuasive than general awareness messaging. These are design principles that industry practitioners are well placed to embed.

[20] HM Treasury, Financial Inclusion Strategy, November 2025, Chapter 6: Financial Education and Capability. [6] Home Office, UK Fraud Strategy 2026-2029, para. 83. [22] Home Office / Ipsos UK (2026). Lived Experiences of Money Muling. Published 16 July 2026.

7. About the Programme

The Future Finance Collaborative Challenge Programme is a structured methodology for bringing together cross-sector expertise to tackle shared challenges in financial services. It uses the Design Council's Double Diamond methodology: a structured facilitation approach that creates space for both divergent problem definition and convergent solution development.

The programme has, over three years, delivered 20 Collaborative Challenges involving 95 participating organisations and 1,400 workshop participants. 95% of participating companies have reported a genuine innovation outcome.

This challenge, Tackling Payment Fraud at Source, was run across three sessions in June 2026. Participants were drawn from financial services, banking, academia (University of Bristol and Cardiff University), and policy. Sessions were hosted at Triodos Bank in Bristol.

The programme was run in partnership between Future Finance UK and FinTech West. This report is published as an open-access output. The full report and supporting materials are available at: future-finance.tech/collaborative-challenge-programme

About Future Finance

Future Finance is a UKRI and ESRC funded project supporting organisations in the UK financial service sector to adopt innovative processes and products, boost their productivity, and improve the accessibility of their services. Through tailored skills training, collaborative opportunities, and social science-led research, supporting organisations in adopting cutting-edge solutions to meet customer needs.

About FinTech West

FinTech West is the representative body for the FinTech ecosystem in the South West of England.

Founded in 2018 and based in Bristol, it brings together financial services, FinTech businesses, technology companies, professional services, universities, investors, regulators and policymakers to connect, collaborate and create opportunity.

Its free-to-join, partner-led community includes more than 5,000 contacts. Website: www.fintechwest.co.uk

Full Reference List

[1] Home Office (2026). UK Fraud Strategy 2026-2029, Annex B: Metrics. Crime Survey for England and Wales (CSEW), year ending September 2025. Available: https://assets.publishing.service.gov.uk/media/69ae77ddc78869bf8eb8a509/fraud-strategy-web.pdf

[2] Home Office (2026). UK Fraud Strategy 2026-2029, Annex B: Metrics. Report Fraud reported losses to Action Fraud, year ending October 2025.

[3] UK Finance (2025), cited in Home Office (2026). UK Fraud Strategy 2026-2029, para. [Section 4.4]: '70% of APP cases start online.'

[4] UK Finance (2025). Half Year Fraud Report 2025, cited in Home Office (2026). UK Fraud Strategy 2026-2029, para. 61-62.

[5] UK Finance (2025). Fraud Report 2025. Investment scam losses rose 34% year on year to £144.4m.

[6] Home Office (2026). UK Fraud Strategy 2026-2029, para. 83. Citing study: 96% of 13-18 year olds transact online; 14% believe they have been defrauded.

[7] Ryder, N. et al. (2026). UK Money Mule Study: analysis of Freedom of Information data across all UK police forces. University of Bristol and Cardiff University. Funded by the Jockey Club Trust.

[8] Home Office (2026). UK Fraud Strategy 2026-2029, paras. 32-39. Online Crime Centre: £31m investment, led by Home Office and NCA.

[9] HM Treasury (2025). Financial Inclusion Strategy. November 2025, p.13. Available: https://assets.publishing.service.gov.uk/media/6909ed8db04a520c5051843f/Financial_Inclusion_Report.pdf

[10] FCA (2022). Consumer Duty. Finalised Guidance FG22/5, July 2022.

[11] Home Office (2026). UK Fraud Strategy 2026-2029, Annex C, para. 4: 'Data fragmentation and sharing barriers.'

[12] Home Office (2026). Call for Evidence: Economic Crime Information Sharing. Published 9 March 2026, closed 18 May 2026. Responses to inform a public-private Data Strategy under Economic Crime Plan 2. Available: https://www.gov.uk/government/calls-for-evidence/economic-crime-information-sharing. No summary of responses published as of July 2026.

[13] Home Office (2026). UK Fraud Strategy 2026-2029, para. 5 and Annex A Delivery Plan: Stop! Think Fraud campaign expanded from 2026.

[14] Home Office / DCMS (2026). UK Fraud Strategy 2026-2029, Annex A Delivery Plan: Online Advertising Taskforce report due Q1 2027.

[15] Home Office (2026). UK Fraud Strategy 2026-2029, Annex A Delivery Plan: Call for Evidence on unauthorised fraud, Q4 2026.

[16] PSR (2024). Mandatory APP Fraud Reimbursement within the Faster Payment System, from October 2024.

[17] Home Office (2026). UK Fraud Strategy 2026-2029, paras. 94-97. Covers FCA analysis of cashing-out; NCA money mule working group; Ipsos research on money muling; Children's Society referral pathways; City of London Police Fraud PREVENT lead.

[18] Home Office (2026). UK Fraud Strategy 2026-2029, paras. 92-93. UK Finance Vulnerable Victim Notification Scheme; Financial Safeguarding Scheme.

[19] Home Office (2026). UK Fraud Strategy 2026-2029, paras. 103-104. Fraud Victims Charter (2027); Report Fraud service.

[20] HM Treasury (2025). Financial Inclusion Strategy, November 2025, Chapter 6: Financial Education and Capability, pp.41-45.

[21] Home Office (2026). UK Fraud Strategy 2026-2029, para. 15. Citing: survey of fraud victims on emotional, physical and behavioural impact.

[22] Home Office / Ipsos UK (2026). Lived Experiences of Money Muling. Published 16 July 2026. Available: https://www.gov.uk/government/publications/lived-experiences-of-money-muling/lived-experiences-of-money-muling

[23] Home Office (2026). UK Fraud Strategy 2026-2029, para. 8, citing HM Government, Economic and Social Cost of Fraud 2023-2024. Available: https://www.gov.uk/government/publications/economic-and-social-cost-of-fraud-2023-to-2024

[24] Home Office (2026). UK Fraud Strategy 2026-2029, paras. 20, 30-31, 45. Organised crime groups' reinvestment of fraud proceeds; scam compounds and forced labour; Prince Group sanctions case study, October 2025.

[25] Revolut Group Holdings Ltd (2026). Consumer Security and Financial Crime Report FY25, p.10, Exhibit 2: APP fraud by platform 2025. Available: https://assets.revolut.com/pdf/Revolut_Consumer_Security_and_FinCrime_Report_compressed.pdf

[26] Home Office (2026). UK Fraud Strategy 2026-2029, para. 60 (Section 4.5: Preventing the abuse of the UK's financial flows. Describes the financial services sector as often the last line of defence in disrupting both unauthorised and authorised fraud.

[27] Data (Use and Access) Act 2025 (c.18), amending UK GDPR Article 6(1)(ea) to introduce 'recognised legitimate interests' as a lawful basis for processing, including fraud prevention, fraud detection and crime prevention. Available: https://www.legislation.gov.uk/ukpga/2025/18/contents