



connecting the future

Unauthorised Fraud in the UK

Call for evidence on unauthorised fraud: criminal methods, drivers, controls and future policy

Home Office

Published 15 July 2026

Response from
The Payments Association

Introduction

The Payments Association (“TPA”) welcomes the opportunity to respond to the Home Office's call for evidence on unauthorised fraud in the UK, published on 15 July 2026 and closing on 7 October 2026. Unauthorised fraud, where payments are made from a victim's account or card without their knowledge or consent, is the largest category of fraud loss in the UK. It touches every part of our membership, from banks and card issuers to acquirers, e-money and payment institutions, wallet providers and the technology and fraud prevention firms that support them.

This response reflects views and evidence from TPA members gathered at a members' evidence session held on 28 September 2026 and through follow-up written submissions, including from an app-based business banking provider, a member that operates a consumer scam-checking service, an e-money institution that provides accounts and payment rails to other financial institutions and a financial crime consultancy drawing on its clients' experience. Contributors included banks and building societies, app-based payment firms, fraud prevention specialists and advisers. TPA's membership holds a diverse range of views, and this response cannot and does not claim to represent the position of every member on every question. Where members' practice or views differ, we say so.

We are grateful to the contributors to this response, which has been drafted by Robert Courtneidge on behalf of TPA's Policy team. We note that the Home Office will share responses with HM Treasury. We welcome that, because the questions raised here about authorisation, authentication and liability bear directly on HM Treasury's current reform of the Payment Services Regulations 2017 (“PSRs”) and on the move of strong customer authentication requirements into FCA rules. We cross-refer to our response to HM Treasury's Modernising Payment Services Regulation consultation where relevant.

We answer the call for evidence's 27 questions below, in order and in the Home Office's own wording, grouped under its seven sections. Where our members do not hold specific evidence on a question, we say so rather than speculate.

The Payments Association is content for the Home Office and HM Treasury to identify it by name as a respondent to this call for evidence.

Emma Banymandhub
CEO
The Payments Association

Executive summary

The Payments Association's five tests for tackling unauthorised fraud

TPA tested the call for evidence against five principles, which members discussed at our evidence session. They frame our detailed answers and underpin the five recommendations in our conclusion.

- **Source-led.** Responsibility should sit where the fraud starts. Most unauthorised fraud begins outside payments: a phished passcode, a hijacked phone number, a fake checkout page or a breached database.
- **Legally clear.** One test should decide whether a payment was authorised: whether the customer consented to it under the PSRs. What the customer did along the way should go to liability, not to the label.
- **Outcomes-based.** As strong customer authentication moves into FCA rules, firms should be judged on fraud outcomes and given a clear path beyond SMS one-time passcodes, while the principle that payments must be authenticated stays in legislation.
- **Intelligence-led.** Data should reach whoever can stop the fraud, in real time, across banks, payment firms, telecoms providers and online platforms, on a clear legal footing that smaller firms can use too.
- **Proportionate.** Every new measure should show that it cuts fraud, and should weigh the friction and cost it imposes on genuine customers, on financial inclusion and on smaller firms.

These tests lead to five recommendations, set out in full in our conclusion: share responsibility along the fraud chain; keep one legal line between authorised and unauthorised payments; authenticate for outcomes; fix how cards are added to digital wallets; and share intelligence in both directions, with mandated participation where voluntary schemes have stalled.

General observations

What the data already show

Unauthorised fraud losses were £703.4 million in 2025, down 5%, while the number of cases rose 11% to 3.81 million. Banks and card companies prevented £1.68 billion of unauthorised fraud in the same year, more than twice the amount lost. Remote purchase (card-not-present) fraud accounted for £423.5 million, or 60%, of losses. Remote banking losses fell 27% to £104.4 million, even though cases rose 11%. Two conclusions follow. Controls work where they are deployed. And the growth is in attacks that trick customers past authentication rather than avoid it, which is where most of the Home Office's questions point.

Unauthorised fraud is a chain, and most of it starts outside payments

Members describe unauthorised fraud as a chain: harvesting credentials, taking over the card or account, and cashing out. Each stage sits in a different sector. Customers are often drawn into the fraud well before any payment is in view, through data shared on social media, fake adverts or a breach. Payment firms see the last stages and bear the loss, but the first stage, which is the least regulated, is where intervention would do most good. As one member put it, financial services see fraud at the end of the chain rather than the start. When one channel is closed, fraud moves to the weakest remaining one, so solutions must land across sectors.

Consistency with the payment services reforms

This call for evidence, HM Treasury's reform of the PSRs and the move of strong customer authentication into FCA rules all touch the same rules on authorisation, authentication and liability. They must produce one coherent answer. In particular, the treatment of payments made by AI agents outside the customer's mandate, which we address under Questions 1 and 6, must be the same in all three. Divergence from the EU on authentication should also be a deliberate choice: the EU is keeping authentication requirements in legislation, and the UK should not drift away from that by accident.

Evidence, not opinion, and alignment with UK Finance

We have brought member data to this response wherever it exists. Many of our members also contribute to UK Finance's response, and we expect our evidence to be consistent with it on the data while reflecting the wider range of firms TPA represents, including smaller payment firms, fintechs and technology providers. We would welcome the opportunity to work with the Home Office on gathering origin-tagged case data across the industry, which would turn the argument that fraud starts upstream into a measured fact.

Response to the call for evidence questions

The call for evidence poses 27 questions across seven sections. Each is reproduced below and answered in order.

Section 1: Criminal methodologies and emerging threats

Q1: What do you consider to be unauthorised fraud?

Unauthorised fraud is a fraudulent payment or transaction made without the genuine account holder's knowledge or consent. It includes cases where a criminal obtains control of an account, card, payment credential or authentication mechanism and uses it to pay without the customer's authorisation. Typical examples are account takeover, stolen cards and devices, and compromised card details, which in turn result from compromised credentials, SIM-swap fraud or social engineering.

We support the Home Office's definition. The legal test that matters, however, is the one in the PSRs: whether the payer consented to the payment transaction. We urge the Home Office and HM Treasury to classify cases by that single test. If the customer did not consent to the payment, it is unauthorised, even if the customer was tricked into sharing a passcode or approving a notification along the way. What the customer did should go to liability, through the gross negligence standard, not to the label.

Members drew two boundaries the definition should recognise. First, payments made under threat of violence, for example being forced to enter a passcode at knifepoint, involve no deception. Some members treat these as a separate crime, such as theft or assault, while still refunding the customer; others record them as authorised fraud, and note that such claims can be very hard to substantiate. Second, theft by someone in a position of trust, such as a carer, a family member or an attorney abusing a power of attorney, is better treated as financial abuse or "friendly fraud". Members regard these payments as unauthorised by the account holder, even though the payment system records them as properly authenticated.

Payments made by AI agents need an explicit rule. Where an agent pays within the customer's instruction, the payment is authorised. Where it goes beyond its mandate, for example by paying a different amount or merchant, there is a strong case that the payment should be treated as unauthorised as against the customer, with liability between the agent provider and payment service providers then following their roles. This is consistent with the approach we have proposed to HM Treasury.

Q2: How does your organisation differentiate unauthorised fraud from authorised fraud, and what sorts of cases do you find it difficult to do so?

Members generally assess whether the customer personally initiated and approved the transaction, alongside the circumstances and fraud indicators around it. If the customer initiated the payment, it is typically treated as authorised fraud; if not, as unauthorised.

Classification is often provisional. Firms usually classify a case at first on the customer's description of the scam, and later investigation can overturn that classification or show that no unauthorised payment took place. The customer may recognise the payments and withdraw the claim, or may have authorised them but reported them as unauthorised, believing that to

be the right way to report the incident. Some cases turn out to be first-party fraud, and many turn out to be authorised push payment scams rather than genuine unauthorised fraud.

The difficult cases are hybrids, where the customer takes an action without intending the payment that follows, or where there is evidence of successful authentication without genuine intent. Members described how they classify the most common ones:

- **Passcode given to a fake bank caller.** A customer phished through a delivery or parking text enters their card details, then receives a call from someone posing as their bank asking for a code “to stop the payments”. The code in fact approves the fraudster's payment. Members treat this as unauthorised: the customer gave the code, but not for the reason they believed.
- **Lost or stolen device.** Payments approved in the victim's app after the device is stolen are generally treated as unauthorised, because the customer had no control of the device. These claims can be hard to substantiate, and some customers then seek reimbursement under the authorised push payment scheme because money left their account, which shows how poorly the boundary is understood by the public.
- **Remote access software.** If the customer does not know the fraudster is moving money through their banking, the payment is unauthorised. If the customer is aware, for example because they believe they are being helped to invest, it is authorised. Members find these among the hardest cases: the customer may enter credentials or approve payments themselves without understanding they are being defrauded.
- **Biometric misuse.** A customer's biometrics may be used to approve a payment without their genuine intent, for example by another person while the customer is intoxicated.
- **Threat of violence; carers and attorneys.** Treated differently by different firms, as described under Question 1. A customer's capacity also matters: a person with an intellectual disability may not be able to give the same level of authorisation.

Members do not all draw the line in the same place. One member sees customers who completed every authentication and authorisation step without understanding that they were authorising a payment: to them, the process looked like something else, because of the design of the scam, a limited understanding of the authorisation process or their own vulnerabilities. These cases are often reported as unauthorised, although the evidence indicates that the customer authorised the payment.

As one member put it, almost every payment is technically authorised by someone; the real question is who authorised it, and on what information. Some cases also start as authorised and end as unauthorised. The boundary is not binary, which is why members support an explicit rule rather than case-by-case labelling. The clarification needed is to the gross negligence standard, so that firms and customers know when sharing a code or approving a notification under sophisticated social engineering does and does not shift liability to the customer.

The stakes of the label are significant. An unauthorised payment must be refunded by the end of the next business day, with the customer's liability capped at £35 unless they acted fraudulently or with gross negligence. An authorised push payment fraud on Faster Payments

or CHAPS falls under the reimbursement requirement up to £85,000, while an authorised card payment has no statutory refund. Inconsistent labelling produces materially different outcomes for victims of the same scam.

Q3: What types of unauthorised fraud have you or your organisation been exposed to?

Members report exposure to: lost or stolen cards and devices; friendly fraud by family members, friends or colleagues; biometric misuse; social engineering that tricks customers into sharing credentials or authentication codes; compromised credentials obtained through phishing and impersonation; account takeover driven by SIM-swap fraud and phone theft; accounts opened and payments made in a victim's name using stolen or copied identity documents; and card-not-present fraud using compromised card details, including through enumeration and card-testing attacks.

Members now see mass credential harvesting through hacks and data breaches as the single biggest enabler of unauthorised fraud, replacing the card skimming that dominated 15 years ago.

A member that operates a consumer scam-checking service reports that the scams leading to unauthorised fraud almost always start with social engineering. Bank impersonation requesting one-time passcodes is very common: the cumulative volume of bank impersonation scams detected by its service rose 163% from the fourth quarter of 2025 to the first quarter of 2026, and a further 28% in the second quarter. Fake e-commerce websites and checkout pages are the other main route: the same member identified a 459% increase in confirmed purchase scams from the first to the second quarter of 2026, and expects the trend to continue through the Black Friday and Christmas period.

Q4: What methodologies do criminals use to commit unauthorised fraud?

Members listed: phishing and smishing; other credential harvesting, including through malware and data breaches; SIM swaps and the exploitation of compromised mobile numbers; account takeover; identity theft, including stolen or copied identity documents, and synthetic identities; digital wallet abuse; AI-enabled impersonation and deepfakes; exploitation of trusted relationships; and the theft of physical cards and devices.

Social engineering is central, and criminals are making it harder to spot. Fraudsters impersonate organisations customers expect to hear from, such as banks, delivery firms and parking providers, and ask for something that feels low-risk, such as a small redelivery fee or a “verification” code that in fact adds the victim's card to a fraudster's digital wallet.

Attacks range from bulk to individual. A convicted fraudster speaking at an industry conference described buying compromised card details in bulk on the dark web and messaging apps, working through them until some succeeded, and targeting cards from countries with weaker authentication. At the individual end, members have seen thefts from gym lockers, where the victim's card is registered to the fraudster's phone and the one-time passcode sent to the victim is read from the preview on their locked phone screen.

The fastest-growing methods defeat authentication rather than avoid it. Account recovery is a further weak point: where changes to passwords, phone numbers or email addresses are not protected by step-up authentication, a fraudster can take control of an account after an initial

compromise. By value, most loss remains online card fraud: remote purchase fraud was £423.5 million of the £703.4 million lost in 2025.

Q5: What evidence do you hold on the scale and nature of first-party fraud within unauthorised fraud, including its prevalence in remote purchase, card, and dispute-related transactions?

Members see significant numbers of suspected first-party claims. One member reports that the most common are claims for reimbursement of gambling losses, which customers say were unauthorised but which were made on the customer's own phone, verified by their own face or fingerprint and made from their usual IP address.

Members draw on transaction monitoring, investigations, disputes, chargeback data and recurring patterns to assess first-party fraud, using indicators such as device information, authentication records, transaction history and previous disputes. They see it most in remote purchases disputed despite evidence that the customer's own credentials or device were used, in card transactions involving family or friends with access to the card, and in disputes where the customer later says they did not recognise a payment. First-party fraud is hard to quantify precisely because it overlaps with genuine unauthorised fraud and friendly fraud, and not every disputed but authenticated transaction is first-party fraud.

Firms in the same payment chain can also reach different conclusions on the same case. A sending bank may treat a case as unauthorised or authorised fraud while the receiving firm assesses it as first-party fraud, concluding that the customer is exploiting weaknesses or information gaps in the payment chain to keep the goods or service and recover the money paid for them. Firms in the middle of the chain often rely on the sending bank's own investigation to identify first-party fraud, and the information they receive can be too limited to assess the typology at all.

False claims exploit the next-business-day refund requirement and inflate headline figures. First-party fraud should be measured separately so that policy rests on an accurate picture of third-party fraud. We would support work by the Home Office and industry to agree a common definition and measure.

Q6: What emerging threats do you anticipate over the next 3-5 years?

Members expect fraud to become more sophisticated rather than fundamentally new. AI will make existing frauds more believable and harder to detect and investigate: where fraudsters once doctored a utility bill with correction fluid and a photocopier, they now generate one with AI. Fraudsters are always early adopters of new ways to pay, so threats will follow whichever payment methods succeed, whether agentic commerce, Open Banking or stablecoins. Members highlighted:

- **AI-enabled social engineering**, including deepfakes, voice cloning and highly targeted scams, with AI agents able to run frauds end to end. AI-generated audio, video and images can also be used to bypass identity verification controls and take over accounts, and depending on the circumstances the same techniques can produce either unauthorised fraud or authorised push payment fraud.
- **Remote-access fraud and manipulation of biometrics and authentication**, making it harder to distinguish genuine customer intent.

- **Synthetic identities and automated fraud at scale.**
- **Agentic payments.** As customers delegate payments to AI agents, fraudsters will target agents and the mandates they hold, and agents themselves may act outside their mandate. Members propose recognising a mandate assurance service, which issues, maintains and attests to an agent's delegated authority, and flagging in the payment message when an agent is involved, so that issuers can apply extra checks. Permissions given to agents must be auditable and traceable, so that it is clear whether an agent acted outside its mandate and where liability sits.
- **Wallet and contactless attacks,** including fraudulent wallet provisioning and relay attacks on contactless cards.

Section 2: Drivers of unauthorised fraud

Q7: What factors are causing or enabling unauthorised fraud to happen?

Members identified these main factors:

- **AI,** which has made it quick and cheap to produce convincing fake websites, messages, documents and reviews at scale.
- **Legitimate channels used to reach victims,** including paid social media adverts and marketing emails, with fake trust signals such as review scores. Customers often hand over card details believing they are buying a holiday or a sofa from a fake advert.
- **Weak authentication and account recovery,** including reliance on SMS one-time passcodes and insufficient step-up checks when credentials change. The security steps meant to protect customers have themselves become targets.
- **Compromised data and phone numbers:** data breaches, phishing, enumeration and card-testing, SIM swaps and number porting. Members cite a 1,055% rise in UK SIM-swap attacks in 2024, from 289 to nearly 3,000 cases.
- **Compromised identity documents and devices:** stolen or copied identity documents, compromised personal devices and the unauthorised disclosure of confidential information, made easier by limited customer awareness of cyber threats and fraud risks.
- **Fraud-as-a-service,** which makes sophisticated tools and stolen credentials readily available.
- **Fragmented intelligence,** so that no single bank, telecoms provider, platform or payment firm sees the whole fraud journey. Firms that sit between the sending and receiving firms often see only what others in the chain report to them.
- **Speed and reach:** real-time payments reduce the time to detect and recover funds, and cross-border networks make investigation and enforcement harder.

Authentication therefore needs to apply across the whole customer journey: not only at login and payment, but when credentials change, a new device is added or other high-risk activity takes place.

Q8: What technologies or digital developments are being exploited to enable unauthorised fraud (for example, digital commerce such as online retail and e-commerce platforms; e-sims, mobile banking and app based financial services)?

Digital commerce is the development most exploited. AI now lets fraudsters build online shops that look entirely legitimate; often the only giveaway is a checkout that redirects to a separate fraudulent page to harvest card details. One member saw clone websites detected by its service rise from negligible numbers in February 2026 to nearly 900 in April. Clone sites of well-known brands reappear on new domains soon after being taken down.

Members also identified: e-SIMs and mobile-number compromise, which undermine SMS authentication and account recovery; remote-access and screen-sharing apps that let fraudsters control customers' devices; instant payment services, which move funds before fraud is detected; remote account onboarding, where stolen or copied identity documents can be used to open accounts in a victim's name; mobile banking and app-based payments; and the provisioning of cards to digital wallets (Question 9). Telecoms providers should verify identity robustly before any SIM swap or e-SIM transfer and send payment firms a real-time signal when one happens.

Q9: What role has the growth of digital wallets (e.g. pass-through wallets and in-device wallets) played in the incidence or nature of unauthorised fraud?

Digital wallets have not created new fraud types, but they have changed the speed, scale and complexity of existing ones, particularly account takeover. Fraudsters now add the victim's card to their own wallet, typically by disguising the provisioning passcode as a routine checkout or verification code, or after taking over the account. One member saw clone websites impersonating a major supermarket surge from May 2026, peaking in June at 277% of May's level. Once the card is tokenised on the fraudster's device, payments are authenticated by that device and can look like genuine customer activity.

Wallets also slow detection. Members who have run fraud teams describe a delay between a wallet payment happening and the card issuer becoming aware of it, which lengthens the time before fraud on the card is spotted, a form of layering on the payment side. Funds can also move rapidly through wallets, making them harder to trace and recover.

The picture is not uniform. One member, which has limited visibility of the payment instruments end users rely on, does not yet have evidence that the growth of wallets has materially increased unauthorised fraud in its own cases.

The weak point is not the wallet but how cards get into it. Once provisioned to the right device, tokenised wallet payments are among the safest ways to pay. Their built-in tokenisation, device binding and multi-factor authentication can reduce some risks compared with traditional payment methods. The fix is at provisioning: friction matched to risk when a card is added to a new device, including clear wording that says a card is being added to a wallet, a cooling-off period or reduced limits for newly provisioned cards, and an instant alert to the cardholder. We recommend an industry standard for provisioning, developed with the card schemes and wallet providers.

Q10: How is artificial intelligence used to enable and prevent unauthorised fraud, and how is this likely to evolve over the next 2-5 years?

Criminals use AI to generate convincing phishing messages, personalise attacks, create fake websites and documents, clone voices, create deepfake video, automate reconnaissance, script social engineering, create synthetic identities and operate at scale. AI is removing the tell-tale signs customers used to rely on, with new patterns emerging almost every week. Reports of suspected AI-enabled fraud to Report Fraud rose 469% between 2023 and 2025.

Defensively, AI is not new: machine learning has been used in transaction monitoring for years, for example to analyse networks of activity. Firms use it to identify unusual transactions, anomalous device behaviour, account takeover, coordinated mule activity and relationships between apparently unrelated accounts, to prioritise investigations, to improve risk scoring models, to strengthen identity verification and to reduce false positives. Generative AI is the new element, and the same technology that makes a convincing deepfake can be used to detect one. Prevention also increasingly depends on tools that assess a message or website at the moment a customer decides whether to trust it. Over the next two to five years, members expect scams to become more personalised and automated, and AI-powered impersonation and deepfake fraud to become more prevalent and harder to investigate, making real-time detection and real-time data sharing more important.

Section 3: Origins of unauthorised fraud

Q11: Where do unauthorised fraud attacks most commonly originate (platforms, devices, networks, geographies)?

Most unauthorised fraud originates outside the payment system. Platforms: fake websites and checkout pages, online marketplaces and paid adverts on social media and search. Devices: stolen and compromised phones and computers, malware and remote-control apps. Networks: phishing links, malicious websites, compromised Wi-Fi, and telecoms networks through SIM swaps and e-SIM transfers. Data: breaches and credential markets. Geographies: fraud originates both domestically and from abroad, and one member reports an increase in device and card theft in London. Payment firms typically see the attack only at the point of cash-out, and attacks often involve several channels rather than one source.

Members are not yet able to tag their unauthorised fraud cases consistently by origin. Intermediaries see even less, as they do not always have visibility of the full fraud lifecycle. We recommend that industry and the Home Office agree a simple origin taxonomy (platform, telecoms, data breach, device) so that firms can record it, and TPA would be glad to coordinate a sample of origin-tagged cases from members as a starting point.

Q12: What evidence is there that criminals use more than one step or channel to carry out unauthorised fraud, and how do these stages interact?

Members' experience is that unauthorised fraud is usually a chain of related activity rather than a single event. One member gives two sequences it sees:

- external bank funding, then a loan or credit drawdown, a card payment, a wallet or e-commerce transaction, a refund or return, and onward movement of funds; and
- account takeover, then the addition of a new beneficiary or payment instrument, a transfer, wallet or card spending, and a refund or onward transfer.

More generally, personal information is first obtained through phishing, social engineering, data breaches, stolen documents or compromised devices, then used to gain access to accounts, pass identity verification checks, open new accounts or make payments. Several channels are usually involved, such as social media, messaging apps, email, websites, telephone calls and digital financial services, although firms that see only part of the chain cannot always reconstruct the whole fraud.

Each event may look normal on its own; the risk only becomes clear when they are analysed as a connected sequence, across accounts, devices, merchants and payment methods. Criminals exploit differences in controls between channels: an account that looks low-risk on one channel may look highly unusual when all channels are combined. Details harvested in one attack are also reused to make the next impersonation more convincing. Because each stage sits in a different sector or channel, a control in one place moves fraud elsewhere rather than stopping it.

Section 4: Barriers to reducing unauthorised fraud

Q13: What are the main barriers to reducing unauthorised fraud?

Members identified:

- **Fragmented data and limited visibility.** No organisation sees activity outside its own walls. Awareness of the information-sharing provisions in the Economic Crime and Corporate Transparency Act 2023 has grown, but there is no central architecture to share intelligence in practice, particularly for smaller payment firms that cannot access the networks larger banks use. Sharing information while maintaining privacy and regulatory compliance remains difficult.
- **Voluntary participation.** Most anti-fraud initiatives are voluntary, which slows them down. Pay.UK's enhanced data sharing will be very useful at the point of payment, but it covers transactional data rather than broader intelligence sharing for horizon scanning, and has moved at the pace of the largest banks.
- **Misaligned incentives.** Liability falls on the customer's payment firm even where the fraud was enabled by a failed identity check at a telecoms provider or a scam advert left on a platform.
- **Speed and sophistication.** Instant payments, increasingly sophisticated account takeover, differences in controls between payment methods, and the difficulty of distinguishing genuine unusual activity from fraud or of identifying the ultimate beneficiary of stolen funds.
- **The human factor.** Fraudsters exploit people who are unfamiliar with fraud risks or do not understand how payment authorisation and security processes work. Customers may not realise how their personal information can be misused or which actions authorise a payment, so they share sensitive information, miss warning signs or believe they did not authorise a payment when they did. Technology helps, but fraudsters adapt and often rely on trust, confusion and lack of knowledge rather than on technical weaknesses.

- **Customer expectations and awareness.** Customers expect convenient, low-friction services, and public awareness of fraud is not sustained: national campaigns have been intermittent.
- **Weak links in authentication,** including continued reliance on SMS passcodes and weak protection of account recovery and device changes.

Q14: What is the most effective way to address these barriers, and which actors are best placed to do so (for example, industry, Government, regulators or other bodies)?

The most effective approach is shared responsibility across the fraud chain. Banks and payment firms are best placed to prevent unauthorised transactions themselves, while Government, regulators and technology and telecoms companies need to address the wider causes and criminal networks:

- **Banks and payment firms** should detect and block suspicious transactions through stronger authentication and real-time monitoring, and develop industry standards for card provisioning to wallets and shared detection models.
- **Technology and telecoms companies,** including social media platforms, online marketplaces and messaging services, should prevent scam messages, websites, adverts and account takeovers, under enforceable duties with a share of losses where they fail, building on TPA's earlier calls on authorised push payment fraud.
- **Digital identity providers and organisations that store personal data** also have a role, since data breaches and compromised accounts are a frequent starting point for fraud.
- **Regulators** should set consistent fraud-prevention standards and outcomes-based authentication rules as strong customer authentication moves into the FCA's rulebook.
- **Government** should mandate participation in key data-sharing initiatives, as Confirmation of Payee was made a condition of using Faster Payments; build the Online Crime Centre into a two-way, real-time intelligence hub open to telecoms providers, platforms and smaller payment firms; fund regular, branded public fraud-awareness campaigns, including in schools; and, with law enforcement, tackle organised fraud and recover stolen funds.

Education should reach the employees of financial institutions, businesses and public bodies as well as consumers, with practical guidance on recognising fraud, protecting personal information, spotting social engineering and understanding how authentication and payment authorisation work.

Q15: How does your organisation balance commercial interest, such as speed and accessibility, with robust security and customer protection?

Members apply friction according to risk rather than to every payment. One member combines selective verification of higher-risk payments, with authentication or confirmation scaled to the risk, with continuous monitoring that looks at amount, timing, the nature of the payment and payee, frequency and velocity, behaviour against the customer's normal pattern, channel, recent context such as a new device, new payee or password reset, and sequences of activity that look legitimate individually but suspicious together. This lets it avoid adding steps to every payment while still intervening where the combination of factors indicates elevated risk.

Friction is a legitimate fraud control, but blanket friction harms genuine customers, damages financial inclusion and can hold back adoption of safer payment methods. A login from a recognised device should not be treated in the same way as a password reset, a new device enrolment or a high-risk payment. Policy should support this risk-based approach and take account of the cost of controls, including false positives, abandoned payments and customers who cannot use app-based authentication.

Q16: What incentives exist to tackle unauthorised fraud, and how might they be strengthened?

Existing incentives are strong for payer payment firms. The PSRs require them to refund unauthorised payments promptly, giving a direct financial reason to invest in detection and authentication. Card scheme rules shift liability between issuers, acquirers and merchants according to authentication, and scheme fraud-ratio thresholds and penalties push acquirers and merchants to manage fraud. FCA systems and controls requirements, the Consumer Duty and customer trust add further incentives. Members point to the authorised push payment reimbursement regime as evidence that liability drives investment in prevention.

The weaknesses are that costs fall mainly on the payer's firm while enablers bear little; there is no shared liability with receiving firms for unauthorised payments, so incentives to control mule accounts are weak; fraud reporting is not standardised, so poor performers are not visible; legal and cost barriers limit real-time data sharing, especially for smaller firms; and low prosecution rates weaken deterrence. If a failed SIM-swap check leads to a £10,000 loss, the customer's payment firm bears it today, and the telecoms provider's incentive to fix its checks is largely reputational.

Members proposed ways to strengthen incentives:

- **Align liability with ability to prevent**, including contributions from non-financial enablers such as telecoms providers and platforms where causation is clear. The EU's new Payment Services Regulation will make platforms liable to payment service providers for scam content they were told about and failed to remove; the UK should go at least as far.
- **Clarify the grey areas**. Clearer, consistent guidance on cases where a customer has shared a passcode or approved a device or notification, so that firms know where losses will fall and invest accordingly.
- **Increase transparency**, through standardised, published fraud, refund and recovery data by firm, linked to supervisory outcomes, and supervisory credit for evidenced controls.
- **Reward good practice**, for example by tiering scheme and acquirer fees according to fraud performance.
- **Enable data sharing** through clear legal gateways and safe harbours, with access for smaller firms, and improve links between industry intelligence and law enforcement.

One member also proposes proportionate cost-sharing between payer and receiving payment firms for unauthorised fraud, to strengthen controls on mule accounts. Other members caution that importing an authorised push payment-style loss split into unauthorised and card fraud

could move cost between payment firms without reducing fraud. We would welcome further work to test whether receiving-firm liability would cut fraud before any such change.

Section 5: Existing measures to address unauthorised fraud

Q17: What steps has your organisation taken to prevent or reduce unauthorised fraud, and how effective have these measures been in practice? Please provide evidence of impact where available, including any data, evaluations or lessons learned.

Industry data show the overall effect of firms' controls: banks and card companies prevented £1.68 billion of unauthorised fraud in 2025, more than twice the amount lost, and remote banking losses fell 27% even as cases rose 11%.

Members' measures include adaptive authentication that increases friction with risk; AI-driven detection of unusual transaction, device and account behaviour; behavioural biometrics using typing, touch and device movement; device binding and passkeys; real-time liveness checks on high-risk transactions; continuous risk monitoring combining device, location, behavioural and transaction signals; detection of compromised devices, malware, screen sharing and repackaged apps; richer transaction telemetry; and manual review of exceptionally high-risk transactions before funds are released.

One member shared six months of data on recall, the share of confirmed unauthorised fraud its controls detected: 45.65% in April 2026, 75.15% in May, 27.00% in June, 27.72% in July, 32.05% in August and 15.45% in September, an average of about 37%. Its lessons are that controls degrade as fraudsters adapt, so models need regular retraining and monitoring, and that recall should be reported alongside false positive rates and customer impact. Those lessons argue for outcome measures in any future regime that capture effectiveness over time, not a single point.

Another member's experience shows the value of intervening before a payment exists. Its AI scam checker lets a customer check a suspicious message or website in under 30 seconds. It has handled nearly 200,000 checks and identified more than 88,000 scams, and at one banking partner it helped prevent £750,000 of losses in a single quarter. Its lesson is that transaction monitoring alone can act only once the victim has already been deceived; prevention has to start with the person, not the payment.

Q18: What are firms' current transaction risk monitoring and analysis capabilities to identify and prevent unauthorised fraud, and how can they be improved?

Firms use real-time transaction monitoring, behavioural reviews, device and location data, authentication records and rules-based detection. Effectiveness comes from combining signals rather than looking at them in isolation: device intelligence can identify a new device, an unusual IP address, location changes or VPNs; behavioural analytics can identify changes in how a customer interacts with their account; and transaction monitoring assesses whether the payment is unusual for that customer.

Members see four improvements: more real-time and behavioural analytics rather than reliance on fixed rules; stronger controls before the transaction, so that changes to passwords, phone numbers, email addresses or recovery details, and new device registrations, trigger step-up authentication; regular testing and retraining of models and thresholds as patterns

change, an area where the FCA has identified weaknesses; and reducing false positives while ensuring suspicious transactions get rapid human review. Capability is also uneven across the market: smaller payment firms need access to consortium data and scheme-level signals, which would close gaps faster than new rules.

Q19: Are there any examples of best practice, in the UK or internationally, that have successfully prevented, disrupted or reduced unauthorised fraud?

Members highlighted:

- **UK:** chip and PIN, and then strong customer authentication and 3-D Secure, which cut counterfeit and card-not-present fraud; tokenisation and device-bound wallets, which make stolen card data far less useful; the industry-funded Dedicated Card and Payment Crime Unit; Cifas and Pay.UK mule tools; and cross-sector action on enablers, such as Ofcom's anti-spoofing rules, the 159 short code and the Online Fraud Charter, though evidence of their impact is still developing.
- **Singapore:** the shared responsibility framework across banks and telecoms providers, with a cooling-off period when new security tokens are activated on a device, real-time alerts, a ban on clickable links in bank messages and a defined waterfall for allocating losses.
- **EU:** transactions authenticated under PSD2 show lower fraud rates, and the new framework adds platform obligations and a legal basis for data sharing.
- **Australia:** a card-not-present fraud framework with merchant thresholds, and the Scams Prevention Framework covering banks, telecoms providers and platforms.
- **India:** mandated card tokenisation, limited customer liability where fraud is reported promptly, and mule detection linked to telecoms data.
- **Sweden:** BankID, a common strong authentication layer that reduces credential-based fraud.

The UK's own data support the point: remote banking losses fell while cases rose. Fraudsters also confirm it. The convicted fraudster described under Question 4 said he targeted cards from countries with weaker authentication, which shows that strong authentication displaces fraud away from where it is applied.

Section 6: Technical standards, controls and authentication

Q20: How effective are current authentication methods (e.g., PIN-based, OTP-based, transaction risk data, biometrics, behavioural analytics)?

Current methods are generally effective, but their strength varies by type of fraud, and they work best combined:

- **PINs and passwords** are useful but vulnerable to theft, phishing and credential compromise.
- **SMS one-time passcodes** are the weakest common factor: they can be intercepted or obtained through phishing, SIM swaps, social engineering or, as members have seen, simply read from a locked phone's notification preview.

- **Transaction risk data** is highly useful when combined with device, location and history.
- **Biometrics** are stronger against credential theft because they tie authentication to the customer, but are increasingly targeted by sophisticated attacks and can be misused, for example while a customer is incapacitated.
- **Behavioural analytics** are particularly effective at detecting account takeover.

Members support moving away from SMS passcodes as a primary control towards device binding, biometrics and passkeys. That move needs a clear path in the FCA's rules, with options for customers who do not have smartphones, so that stronger authentication does not exclude them.

Q21: What weaknesses in technical standards and regulatory requirements are most commonly exploited?

Members identified:

- over-reliance on passwords, PINs and one-time passcodes that can be stolen or tricked from customers, and authentication messages that do not tell the customer clearly what they are approving, such as adding a card to a new wallet;
- default phone settings that display the content of one-time passcode messages on a locked screen, allowing a thief with the phone but not its passcode to complete card registration;
- insufficient step-up authentication for account recovery, credential changes and new device registration, and weak identity checks for SIM swaps and e-SIM transfers;
- weak or slow risk monitoring, and limited data sharing between banks and other organisations;
- rules that do not keep pace with new technology; and
- cross-border gaps, where fraudsters operate outside the UK's regulatory reach.

Prescriptive authentication rules have also made it harder for firms to adopt better methods. As strong customer authentication moves into FCA rules, the test should be whether outcomes improve, not whether a prescribed method was used. But the principle that payments must be authenticated should remain in legislation. It underpins card payments, consent in Open Banking and, increasingly, the permissions customers give to AI agents. Removing it from statute would also put the UK out of step with the EU.

Q22: What additional standards, safeguards or controls would improve resilience against unauthorised fraud?

Members would prioritise:

- **Authentication:** device binding and dynamic linking of authentication to the amount and payee; step-up checks, short delays and alerts when a new device or token is registered, including an industry standard for provisioning cards to wallets; phishing-resistant methods such as passkeys and biometrics in place of SMS passcodes; and tighter account recovery and SIM-swap checks.

- **Device settings:** phone manufacturers and operators should hide the content of security messages on locked screens by default.
- **Detection:** real-time behavioural analytics to spot account takeover and remote-access tools, and cross-firm network analysis, with receiving firms screening inbound payments for mule activity.
- **Customer controls:** easy limits, payment locks and instant alerts with a “this wasn’t me” option, and proportionate holds on high-risk payments with safeguards for vulnerable customers.
- **Ecosystem:** common fraud data standards and legal gateways for real-time sharing; anti-spoofing, real-time SIM-swap alerts to payment firms and faster takedown of phishing sites; minimum fraud controls for merchants, wallets and other third parties; and faster breach notification so that compromised credentials can be reissued.
- **Governance:** outcomes-based FCA authentication rules that accept passkeys and device binding; liveness and deepfake-detection standards for voice and face checks, set with industry; independent testing and cross-industry incident playbooks; and strong staff verification to resist social engineering.

Q23: How effective are current digital identity controls (including biometrics) in preventing unauthorised fraud?

Biometric and device-bound controls provide a strong additional layer. One member has introduced a selfie check for potentially suspicious transactions, triggered by risk indicators such as risk bands, new payees, cooling-period limits, recent biometric changes and machine learning models of payee risk. Where the live selfie does not match the customer’s verified identity, the transaction is held and escalated for fraud review, and further payments to that payee are blocked until the investigation is complete. The member prefers this to knowledge-based questions because the selfie is already collected at onboarding. It is measuring effectiveness through fraud recall, true-positive and automatic approval rates, completion rates for legitimate users, complaints and drop-off, and review time and accuracy, but cannot yet quantify the impact definitively.

The effectiveness of biometric controls is now being tested by deepfake voice and video aimed at verification and liveness checks. The same technology that creates convincing deepfakes can help detect them, and liveness standards should be developed with industry so that biometric controls keep pace.

Section 7: Future policy and regulatory intervention

Q24: What options should Government consider to close vulnerabilities and strengthen defences?

Government should strengthen the wider fraud ecosystem while leaving firms flexibility to develop proportionate, risk-based controls. Members would prioritise:

- enforceable fraud-prevention duties on telecoms providers and online platforms, with a share of losses where they fail;

- mandated participation in key data-sharing initiatives, and a clear legal basis and central architecture for real-time intelligence sharing that smaller firms can use, including making the Online Crime Centre a two-way hub;
- regular, branded, Government-funded public fraud-awareness campaigns, including in schools, rather than intermittent ones;
- implementing Ofcom's fraudulent advertising duties as planned, faster takedown of phishing and clone sites, and stronger controls on number spoofing;
- working with phone manufacturers and operators to hide security codes on locked screens by default; and
- keeping the principle that payments must be authenticated in legislation while the FCA sets the detailed rules.

Any new requirements should be proportionate and supported by clear standards and effective data-sharing frameworks.

Q25: Which regulatory levers or industry standards could most effectively reduce unauthorised fraud?

The most effective levers would be outcomes-based FCA authentication rules, including dynamic authentication that does not rely on SMS passcodes when fraud is suspected; an industry standard for wallet provisioning; real-time SIM-swap signals from telecoms providers; and a clear legal basis for real-time data sharing. One member also proposes requiring merchants to store only tokenised card credentials, to reduce the value of stolen card data.

Every lever should be judged by whether it cuts fraud. Levers that only move cost between firms, or that prescribe a single technology where outcome standards would do, risk slowing the adoption of better controls without reducing losses.

Q26: What future interventions are in development across industry to tackle unauthorised fraud? Please include examples such as new technologies, tools, or approaches to identify or prevent fraud.

Members are developing or deploying:

- passkeys and FIDO-based, device-bound authentication replacing SMS passcodes;
- behavioural biometrics and device intelligence to detect account takeover and remote-access tools;
- AI and graph analytics for real-time scoring, mule network detection and spotting synthetic identities;
- network tokenisation for e-commerce and stored cards, to devalue stolen card data;
- deepfake and liveness detection for onboarding and call centres;
- real-time AI tools that assess a message or website at the point a customer decides whether to trust it;
- privacy-enhancing technologies, such as federated learning, to share fraud signals without exposing customer data, and consortium intelligence models such as the Australian Financial Crimes Exchange;

- telecoms signals such as SIM-swap and number verification APIs; and
- customer-controlled safeguards such as payment locks and trusted devices, and automated takedown of phishing sites and spoofed numbers.

Pay.UK's enhanced data sharing will begin with a first cohort next year that includes a mix of major banks, challengers and fintechs, which members welcome. Research on agentic AI fraud is also under way among members but has not yet produced conclusions. We would welcome the opportunity to bring members developing these tools to meet the Home Office.

Q27: Are there any further views, evidence or data relevant to unauthorised fraud that have not been covered in this questionnaire?

We would highlight three points. First, alignment: this call for evidence, HM Treasury's reform of the PSRs and the FCA's new authentication rules must give one answer on what counts as authorised, how authentication is judged and where liability falls, including for payments made by AI agents. Second, cross-sector collaboration: unauthorised fraud evolves through compromised credentials, digital wallets and social engineering, and controls need to adapt quickly across financial institutions, technology companies and telecoms providers, not within payments alone. Third, proportionality: every new measure should be tested for whether it cuts fraud and for the friction and cost it imposes on genuine customers and smaller firms. TPA would welcome continued engagement with the Home Office, HM Treasury and the FCA, including through its Financial Crime, Agentic Commerce and Financial Inclusion working groups.

Conclusion: five recommendations

Drawing together the answers above, if TPA were to make only five recommendations to the Home Office and HM Treasury, they would be:

- 1. Share responsibility along the fraud chain:** give telecoms providers and online platforms enforceable fraud-prevention duties, with a share of losses where they fail, so that responsibility sits where the fraud starts.
- 2. Keep one legal line:** let the PSRs consent test decide whether a payment was authorised, clarify the gross negligence standard for socially engineered cases, and set explicit rules for hybrid cases such as approved wallet notifications, remote access and payments made by AI agents outside their mandate.
- 3. Authenticate for outcomes:** keep the principle that payments must be authenticated in legislation, and let FCA rules judge firms on fraud results and give them a clear path from SMS passcodes to device-bound, passkey, biometric and behavioural methods, with options for customers without smartphones.
- 4. Fix provisioning, not wallets:** develop an industry standard for adding cards to new devices, require real-time SIM-swap signals from telecoms providers, and hide security codes on locked phone screens by default.
- 5. Share intelligence in both directions:** mandate participation in key data-sharing initiatives, give real-time sharing a clear legal and practical footing through the Online Crime Centre with smaller firms included from the start, and fund sustained public awareness campaigns.

TPA and its members stand ready to support the Home Office and HM Treasury as this work progresses, and would welcome the opportunity to discuss any of the points raised in this response in more detail.

About The Payments Association

The Payments Association is for payments institutions, big and small. We help our members navigate a complex regulatory environment and facilitate profitable business partnerships.

Our purpose is to empower the most influential community in payments, where the connections, collaboration and learning shape an industry that works for all.

We operate as an independent representative for the industry and its interests, and drive collaboration within the payments sector to bring about meaningful change and innovation. We work closely with industry stakeholders such as the Bank of England, the FCA/PSR, HM Treasury, Pay.UK, UK Finance and Innovate Finance.

Through our comprehensive programme of activities for members and with guidance from an independent Advisory Board of leading payments CEOs, we facilitate the connections and build the bridges that join the ecosystem together and make it stronger.

These activities include a programme of digital and face-to-face events including our annual PAY360 and FC360 conferences, our PAY360 Awards dinner, PA@The City, CEO round tables, webinars, working group events and training activities.

We run focused stakeholder working groups spanning Agentic Commerce, Cross-Border, Digital Currencies, ESG, Financial Crime, Financial Inclusion, Merchant Payments, Open Banking, Regulatory, and Payments Infrastructure. The volunteers within these groups represent the collective view of The Payments Association members at industry-critical moments and work together to drive innovation in these areas.

Our Payments Intelligence team and our working groups aim to produce regular thought leadership for our membership and beyond. These include data-driven reports, articles, video interviews and podcasts. We also undertake policy development and government relations activities aiming at informing and influencing important stakeholders to enable a prosperous, impactful and secure payments ecosystem.

See www.thepaymentsassociation.org for more information.

Contact natasha.healy@thepaymentsassociation.org for assistance.