Which?
2 Marylebone Road
London NW1 4DF
020 7770 7000
which.co.uk

7 October 2026

Consultation response

Which? response to Home Office's 'Unauthorised fraud in the UK call for evidence'

Introduction

Which? welcomes the opportunity to respond to the Home Office's call for evidence on unauthorised fraud. In tackling this evolving threat, we strongly encourage the Home Office to closely align its work with related activity being taken forward by other government departments and regulators, such as HM Treasury's consultation on modernising payment regulation.

As the UK's consumer champion, Which? has a long-established role in investigating consumer harms, exposing fraud trends, and advocating for robust protections. This response addresses the specific questions where we have robust evidence and consumer insights to share. In addition, the **Annex** includes key findings in relation to unauthorised fraud from our fraud victim survey (conducted June 2026).

Answers to questions

Q1 What do you consider to be unauthorised fraud?
Q2 How does your organisation differentiate unauthorised fraud from authorised fraud, and what sorts of cases do you find it difficult to do so?

We answer Q1 and Q2 together.

- **Consent -** The Payment Systems Regulator (PSR) defines authorisation as where the payer has given 'explicit consent' to the execution of a payment transaction. Where victims inadvertently share one-time passcodes (OTPs) or confirm push notifications in banking apps, this may not always be explicit consent. For example, victims can be coached into approving card payments in their banking apps in the belief that they are securing their accounts. A victim called Richie came to Which? after losing over £30,000 to bank impersonation scammers. He had been groomed into approving more than 20 virtual debit card payments in his app. However, each card payment was triggered by scammers who had stolen his card details, not him. Richie did not enter his own card details or visit any of the merchants himself. He thought he was blocking each transaction in his app. He did not willingly and knowingly consent to these payments yet his bank considered them to be authorised and did not reimburse him.

- **Unauthorised recurring payments (subscription scams)** set up as continuous payment authorities (CPAs) have become one of the most common threats reported to Which?. Consumers can cancel unwanted subscriptions by contacting their card providers, but they may struggle to get refunded for payments already taken because providers see these as authorised transactions. Card providers can often fail to acknowledge that the 'authority' is only gained through misleading adverts and other underhand tactics, with consumers in many cases clicking on a link to gain more information but being wholly unaware that in doing so they are agreeing to a payment, or recurring payments. It can be impossible for consumers to prove this is the case and to get money refunded.

- **Complex fraud cases:** Scams involving malware and other sophisticated tactics can result in banks telling unauthorised fraud victims that they won't be refunded because they can't find evidence of compromise. In one such case reported by Which?, a bank refused to refund over £6,000 because the payments were made from his registered device and verified by the correct passcode. It transpired that the victim had inadvertently downloaded banking malware which gave scammers remote access to his device. He was only refunded because Which? intervened. In another case, a victim was accused of negligence by his bank when he reported £4,000 in unauthorised debit card transactions. The payments were apparently made in person, in Dubai, while the victim was in London. Which? spoke to experts about a plausible explanation and was told this was likely a relay attack. It was only when Which? challenged HSBC on the geographic impossibility of being on two continents at the same time that the bank issued a full refund and apology.

- **No unauthorised fraud reimbursement data:** UK Finance does not publish a breakdown of reimbursement data for unauthorised fraud or authorised fraud outside of authorised push payments (bank transfers) in its annual fraud report so there is limited insight into how many disputed charges are refunded.

Q4 What methodologies do criminals use to commit unauthorised fraud?
Q6 What emerging threats do you anticipate over the next 3–5 years?

We answer Q4 and Q6 together.

- **Social engineering:** UK Finance said in its 2025 report that record-high levels of card-not-present (CNP) fraud were driven by the increased sophistication of social engineering techniques to acquire one-time passcodes (OTPs) from victims. Which? regularly comes across examples where fraud victims have been manipulated into sharing OTPs with impersonation scammers. However, it's important to remember that consumers' card details are often initially compromised through no fault of their own, such as via phishing, data breaches and malware-infected browsers, websites, or point-of-sale systems.

- **Smishing** (phishing delivered via SMS and other forms of messaging) has become a core driver of industrialised fraud, linked to global criminal networks. Consumers are known to be more trusting of text alerts compared to email. Fraudsters are reportedly shifting from traditional SMS to online messaging apps iMessage (Apple) and RCS (Google). Though users may not distinguish between online messaging apps and mobile

messaging services, they are governed by different regulations, i.e. the Communications Act for SMS and the Online Safety Act for online messaging apps. Unlike mobile operators, Apple and Google don't tend to work with third party security firms and they don't share fraud intelligence with banks. They are also not subject to the same anti-fraud monitoring, data-sharing protocols, or scam reimbursement duties as regulated financial institutions.

- **Email phishing** remains a persistent and widely used tactic by criminals alongside smishing. Despite advanced email filtering by providers, fraudsters continue to send deceptive emails mimicking trusted brands and institutions to harvest personal and financial details, credentials, or authentication codes. As highlighted in Which? advice on spotting email scams, email phishing attacks frequently rely on urgent language, suspicious links, and impersonal greetings to deceive consumers.

- **Rogue advertising:** Subscription scams are a persistent problem and one that we expect to thrive as rogue merchants aren't always reported or investigated. Card providers mistakenly see these as authorised payments because they fail to acknowledge that their customers did not give explicit consent to the Continuous Payment Authority (CPA). Scam subscriptions reported to Which? are largely driven by misleading and/or fraudulent online advertising such as fake social media competitions and camouflaged adverts. However, payment providers have limited to no insight into this tactic.

- **Micro-fraud (low value, high volume):** Remote purchase or CNP fraud reached record highs in 2025. The average transaction loss has fallen from £300 to £132 over the past decade, though they still represent significant sums lost to criminals and the cumulative impact on low-income consumers leads to severe distress, debt, and overdraft charges. Small losses can go unnoticed or unrefunded due to reporting friction.

- **In-person card fraud:** Though not common, we do occasionally get reports of unauthorised fraud involving physical coercion. One recent victim described being scammed by a London pedicab operator who physically grabbed his hand and used it to authenticate a £750 Apple Pay transaction. At present, mobile wallets offered by Apple and Google do not feature transaction limits – unlike contactless payments made by a physical card – because transactions are deemed to be authorised via biometric authentication. In addition, they do not allow users to set personalised transaction limits. This exposes consumers to some risk in terms of coercion and misplaced trust when a terminal is concealed or not clearly visible.

- **Open banking fraud:** As merchants encourage payments initiated through open banking eg to avoid card scheme fees, fraudsters may pivot toward hijacking these transactions, where consumer rights and protections are far less established. The June 2026 Fraud Report from Open Banking Limited reveals that while total open banking fraud rates (including both authorised and unauthorised fraud) remain below wider industry benchmarks by volume, they increased during Q1 2026. The report also notes that *"Newer scam sophistication increasingly blurs the line between authorised and unauthorised fraud, where it is unclear at the point that the victim loses control of their accounts or their funds".*

Section 2: Drivers of Unauthorised Fraud

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

We answer Q7 and Q8 together.

- **Poor cybersecurity practices:** Weak security processes operated by businesses – such as permitting weak or default passwords, failing to use two-factor authentication (2FA), or failing to evolve anti-fraud protections – leave customer accounts vulnerable to compromise. When companies fail to secure their platforms properly, fraudsters can easily break in, steal stored payment details, or take over accounts to carry out unauthorised transactions and fraudulent purchases without the victim's knowledge. As we have highlighted in our investigations into corporate cybersecurity standards, even major consumer-facing firms often fall short of basic security best practices, creating significant blind spots that directly fuel unauthorised fraud. This failure to evolve is particularly evident in the continued reliance on SMS-based One-Time Passcodes (OTPs) for multi-factor authentication (MFA) by some firms, which runs counter to guidance from the National Cyber Security Centre. As Which? has highlighted, SMS is an inherently insecure channel that is highly susceptible to being intercepted, spoofed, or hijacked by cybercriminals through tactics like SIM-swapping.

- **Artificial intelligence** (including real-time voice cloning, visual deepfakes and automated phishing generators) has dramatically lowered the skill barrier for criminals, serving as a powerful driver for unauthorised fraud. As Which? investigations have highlighted (such as our reporting on global AI investment scams and advice on how to spot and avoid AI scams), AI removes traditional indicators of scams – such as poor grammar or unconvincing imagery- enabling fraudsters to deploy hyper-realistic deepfake endorsements, video ads, and sophisticated phishing messages at scale. These tools are routinely used to harvest consumer credentials, compromise accounts, and deceive victims into granting criminals unauthorised access to financial accounts and digital services.

- **Sim-swap attacks:** Which? case studies suggest mobile networks miss fraud indicators such as requests linked to unusual IP addresses and failed or persistent attempts to change sensitive account information. One victim waited 10 days to recover their mobile number, putting them at serious risk of fraud (Ofcom says it doesn't set timeframes for networks to recover phone numbers in Sim-swap fraud cases, as every individual case is different). As mobiles are now the primary gateway to finances, mobile networks must think more like the best performing banks and beef-up their defences**.**

- **Rogue merchant acquirers:** UK Finance said in its 2025 fraud report that 80% of all CNP fraud is e-commerce, with 75% of that occurring at a merchant acquired outside of the UK. While not included in the 2026 fraud report, the UK Finance press office confirmed to Which? that 80% of all CNP fraud related to e-commerce, with 77% of that occurring at a merchant acquired outside of the UK (relates to fraud reported in 2025). Merchant acquirers have clear due diligence obligations when partnering with a

business. Visa and Mastercard should fine and ultimately ban merchant acquirers that fail to carry these out. In addition, a lack of transparency about the identity of these merchant acquirers makes investigating fraud extremely difficult. Consumers' bank statements sometimes contain confusing transaction codes, such as Pyd*tekxtart.com and TFR*VBudgetbloke.co, or country codes like CYP and IRL for Cyprus and Ireland respectively. But these are not standardised references since the merchant and payment processor can agree on the format of such references, rendering them meaningless to consumers. While Continuous Payment Authorities (CPAs) are governed by the Consumer Contracts Regulations 2013, banks are only obliged to stop payments if requested, and are not required to supply details of other actors in the chain as the customer's contract is with the merchant rather than the acquirer.

- **Screen-sharing and remote access tools:** Fraud may involve legitimate tools being abused by scammers, including remote-access software and screen-sharing tools (see WhatsApp screen-sharing scam warning, Which? Sept 2026), yet consumer awareness remains low. In a survey of 8558 current account customers (Aug/Sept 2026), 27% said they had never heard of remote access and screen-sharing software scams. Of the rest, only 23% said their bank had warned them about this and 46% said they heard about it elsewhere.

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?

- **International organised crime** groups impersonate well-known brands and retailers to steal card details and OTPs sent via text. Victims are urged to click on links (from malicious emails, texts, adverts and user-generated posts) to visit copycat websites asking for their card details. If this triggers a security check from their card provider, such as a one-time passcode (OTP) sent via text, they will enter this on the scam website, assuming they are authorising a genuine payment. The fraudster then uses the OTP to complete the digital wallet setup on their own device, free to make both online and in-store payments.

- **Apple and Google** say that the card issuer is ultimately responsible for approving or rejecting digital wallet transactions and adding cards to wallets. But we think banks could do more to prevent digital wallet fraud including: helping customers spot fake phone calls [only a handful of providers offer some form of caller verification]; detecting anomalous activity such as new devices or locations linked to customer accounts; and intervening or sharing this information to help customers flag unauthorised spending. Digital wallet controls are also lagging behind. Many banks now allow you to view, manage and 'untrust' devices linked to your online banking; however, we aren't aware of any banks that let you do the same for digital wallets linked to your bank cards. They should also make it hard for scammers to register card details on their own device, yet most rely on OTPs sent by text message.

- **SCA**: Under the National Payments Vision, the government intends to remove strong customer authentication (SCA) rules from the Payment Services Regulations 2017 in favor of a flexible, "outcomes-based approach." While banks and fintechs may argue that rigid SCA creates checkout friction, there should be a minimum level of mandatory

friction for high-risk actions such as a card being paired with a new device or digital wallet (and subsequent transactions).

Q.16 What incentives exist to tackle unauthorised fraud, and how might they be strengthened?

Under Regulations 72 and 75 of the Payment Services Regulations 2017, Payment Services Providers (PSPs) must refund victims of unauthorised transactions by the end of the next business day unless they can prove fraud or gross negligence. This financial liability is intended to incentivise investment in prevention tools like real-time transaction monitoring and automated fraud blocking.

In practice, however, PSPs can improperly apply the 'gross negligence' exception and erect administrative hurdles to avoid or delay having to make statutory refunds. For instance, firms can issue template rejections claiming credential or OTP usage proves gross negligence, attempting to shift the burden of proof onto consumers. This directly contradicts Financial Ombudsman Service (FOS) guidance, which establishes that gross negligence is a high bar requiring conscious, reckless disregard for security - far beyond falling victim to social engineering or phishing.

Which? research shows only 49% of unauthorised fraud victims receive immediate full refunds, with some waiting up to four months due to bank delays. FOS decisions confirm a pattern of banks misapplying the gross negligence exception:

- Remote access scam: In decision **DRN-5461457**, the Ombudsman held that being manipulated into downloading remote access software or sharing security codes during a social engineering scam does not meet the high threshold for gross negligence.
- QR code refund scam: In decision **DRN-4949831**, the Ombudsman ruled that interacting with deceptive sites or QR codes falls short of gross negligence, reiterating that technical authentication does not prove deliberate or extraordinarily reckless conduct.
- Stolen phones: In decisions such as **DRN-3597000** and **DRN-4113677**, the Ombudsman confirmed that following physical device theft or passcode shoulder-surfing, the statutory burden of proof rests strictly on the PSP to prove gross negligence rather than simply proving credential usage.

To ensure rules effectively protect consumers and better achieve their aim of driving prevention of unauthorised fraud, the existing rules about timely refunds of money lost to unauthorised transactions (e.g. Regulations 72 and 75 of the Payment Services Regulations) should be more strictly enforced. Specifically, the PSR and FCA should undertake proactive monitoring of firms' activities and issue penalties to firms that seek to avoid their obligations.

Annex - Which? fraud victim survey

A 2026 Which? report examined the experiences of UK fraud victims, drawing on data from a survey of 1,501 individuals who suffered financial losses. The headline findings, covering both authorised and unauthorised fraud, feature in the article *Scammers are thriving on Meta's social media platforms*, but below are more detailed findings from the survey on unauthorised fraud:

- 44% of respondents had their personal information stolen and 16% had their physical card, mobile or other device stolen (both unauthorised fraud), whilst 35% sent money to a fraudster and 5% selected 'other';
- Amazon was predominantly associated with unauthorised fraud, while Facebook and WhatsApp were heavily associated with authorised fraud,
- Most unauthorised fraud victims (60%) said they or their bank noticed an unauthorised payment or credit application, while 9% said it was online (social media, search engine, online marketplace, online advert or article), 6% said telephone, 6% said text and 3% said messaging app (e.g. WhatsApp, Signal, Telegram, Viber), when asked 'How did you first come across the fraud that resulted in you losing money?';
- Of the unauthorised fraud victims who said they encountered the fraud by call or text, 64% said it involved number spoofing, where the Caller or Sender ID appeared to belong to a legitimate organisation;
- In our survey, reimbursement rates were significantly higher for victims of unauthorised fraud than for those of authorised fraud, though they did not match the 98% reimbursement rate regularly quoted by industry (UK Finance, 2025);
- Nearly half (49%) of unauthorised fraud victims managed to get all of their money back, which is more than double the rate for authorised fraud victims (21%);
- Unauthorised fraud victims are also far more likely to recover at least some of their losses (68%) compared to authorised fraud victims (37%);
- Victims of authorised fraud are more than twice as likely to be left empty-handed. Over half (55%) of authorised fraud victims did not get any money back, compared to 21% of unauthorised fraud victims;
- There were no notable differences between authorised and unauthorised fraud victims for those who are still in the process of getting their money back or are in dispute;
- When we asked fraud victims if they had changed any financial habits as a result of being defrauded, unauthorised fraud victims were more likely than authorised victims to say they had set up a lower limit for contactless payments and started checking their bank accounts more frequently.

About Which?

Which? is the UK's consumer champion, here to make life simpler, fairer and safer for everyone. Our research gets to the heart of consumer issues, our advice is impartial, and our rigorous product tests lead to expert recommendations. We're the independent consumer voice that works with politicians and lawmakers, investigates, holds businesses to account and makes change happen. As an organisation we're not for profit and all for making consumers more powerful.