



Annual Fraud Report 2026

In partnership with



Contents

Our Fraud Data	4
UK Finance Foreword	5
The Industry Response	7
BioCatch/Nasdaq Verafin Foreword	10
UK Finance Insight	12
Unauthorised Fraud Summary	20
Unauthorised Card Fraud	21
Analysis by Unauthorised Card Fraud Case Type	23
Further Card Fraud Analysis	27
Unauthorised Cheque Fraud	30
Unauthorised Remote Banking Fraud	31
Authorised Push Payment (APP) Fraud	33
APP Fraud Enablers	34
Further Analysis of the APP Fraud Data	36
Authorised Push Payment Fraud – Payment Type	45
Authorised Push Payment Fraud – Payment Channel	46
Our Fraud Data	47
Appendix	49
Contributing Members	51



UK Finance is the collective voice for the banking and finance industry. Representing more than 300 firms across the industry, we're a centre of trust, expertise and collaboration at the heart of financial services. Championing a thriving sector and building a better society.

We represent our members by providing an authoritative voice to influence regulatory and political change, both in the UK and internationally. We also act as advocates on behalf of members to both media and customers, articulating the industry's achievements and building its reputation. We offer research, policy expertise, thought leadership and advocacy in support of our work.

The Economic Crime team within UK Finance is responsible for leading the industry's collective fight against economic crime in the UK, including fraud, anti-money laundering (AML), bribery and corruption and cyber-enabled fraud. UK Finance seeks to ensure that the UK is the safest and most transparent financial centre in the world - thus creating a hostile environment for criminals by working with members, law enforcement, government agencies and other sectors.

Our Fraud Data

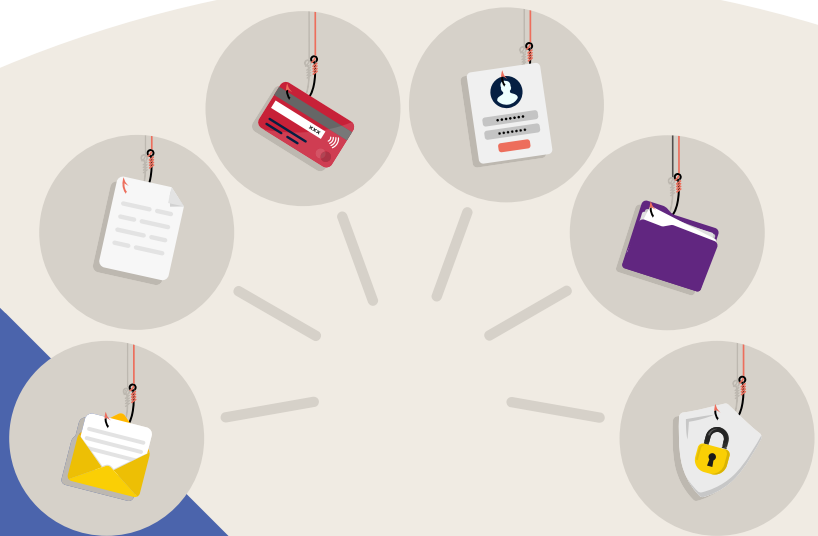
UK Finance publishes both the value of fraud losses and the number of cases. The data is reported to us by our members which include financial service providers, credit, debit and charge card issuers, and card payment acquirers. Each incident of fraud does not equal one person being defrauded but instead refers to the number of cards or accounts defrauded. For example, if a fraud was carried out on two cards, but they both belonged to the same person, this would represent two instances of fraud, not one.

All fraud loss figures, unless otherwise indicated, are reported as gross. This means the figures represent the total value of fraud including any money subsequently recovered by a bank.

All case volumes, unless otherwise indicated relate to only those cases where a financial loss has been suffered – if there was a fraudulent attempt which was not successful for any reason then it will not be classed as a ‘confirmed case’.

Some caveats are required for the tables in the document.

- Comparable authorised fraud data is not available prior to 2020.
- The sum of components may not equal the total due to rounding.
- Data series are subject to restatement, based on corrections or the receipt of additional information.



UK Finance Foreword

Fraud remains the most prevalent crime in the UK and is becoming increasingly sophisticated and internationally coordinated. The scale of the threat and the criminal nature of it damages our economy at a time when we need economic growth. The harm extends well beyond financial losses though: it damages livelihoods, affects victims' mental health and erodes trust in the systems designed to keep customers safe.

Our 2025 data reveals the scale of the threat and the fact the problem is not going away. On average eight people were defrauded every minute, with almost £2,500 lost in that same minute. Fraud operates on an industrial scale, moving fast and adapting quickly.

The UK's financial sector is a global lead in the fight against fraud, but we cannot remain the sole line of defence. In 2025 alone, banks prevented £1.68 billion in unauthorised payment fraud, equivalent to 70p in every £1 of attempted attacks. Despite this £1.28 billion was stolen through various forms of payment fraud.

Our 2025 data also point to significant shifts in Authorised Push Payment (APP) fraud. On the one hand losses from invoice and mandate scams, CEO fraud, and impersonation scams fell to record lows, reflecting the impact of continued industry investment in fraud prevention and customer education and awareness. By contrast, losses from frauds that frequently originate online, where people are manipulated into making payments for seemingly legitimate goods, services, or opportunities - including purchase, investment, and romance scams - reached their highest levels on record. This shows that the tactics criminals deploy evolve and so we need to do more to tackle it.

There is a clear asymmetry of liability in the UK's fraud landscape. Banks fund major prevention initiatives and are the only sector required to reimburse customers, while other sectors continue to profit from fraudulent activity on their platforms.

Voluntary measures have delivered inconsistent results, and technology and telecommunications companies should face responsibilities that match the role their platforms play in enabling scams, including stronger incentives to detect and stop fraud earlier. Our latest data shows that 66 per cent of APP fraud begins online and a further 17 per cent via telecoms.

The Government's 2026 Fraud Strategy was an important step in recognising the scale of the challenge. But, as outlined in our recent 'Plan for Growth: from Strategy to Delivery', it must now turn that recognition into enforceable obligations across the sectors where fraud originates.

Firms in these sectors should contribute financially, as well as share expertise, intelligence and capability to support proactive fraud prevention. Alongside that we have set out two areas which we believe would make a tangible difference:

- The government should legislate to mandate seller verification and secure payment protections on online marketplaces, closing loopholes that fraudsters exploit at scale.
- Ofcom should move swiftly through its Online Safety Act consultation to introduce tougher, more proactive fraud prevention duties. Proportionality must not become a loophole: the largest platforms, where the volume and value of fraud are highest,

should face the strongest obligations. Ofcom must use the full force of its powers to hold social media companies accountable for the fraud that flourishes on their platforms.

We are now over 18 months since the introduction of the Payment Systems Regulator's (PSR) APP reimbursement rules. These have improved outcomes for victims, with 88 per cent of in scope APP losses being reimbursed in the first year. Reimbursement is important, but it is not stopping the fraud. The money stolen still flows to serious and organised crime gangs, undermining national security and weakening the UK's long-term prosperity.

Without shared responsibility, the UK will not reduce fraud at scale.

The financial services industry has demonstrated what coordinated action can achieve. Initiatives such as Take Five to Stop Fraud campaign, the Banking Protocol and the Dedicated Card and Payment Crime Unit (DCPCU) - a specialist fraud police unit funded by the sector which in 2025 prevented over £273 million from being stolen from the public and disrupted 157 serious and organised criminals - show what is possible when prevention, disruption and victim protection work together.

The path forward is clear: banks, tech platforms, telecoms providers and law enforcement each have a role to play, and the system will improve only if responsibility is shared in practice.

The UK cannot afford delay: the longer these gaps remain, the longer criminals will exploit them.



Ruth Ray
Managing Director,
Economic Crime,
UK Finance

The Industry Response

The financial services industry is central to protecting customers from fraud and safeguarding the UK's security, prosperity and reputation. In 2025, its targeted prevention work and sustained investment in technology and security stopped £1.68 billion in unauthorised fraud from being stolen. With deep expertise and system knowledge, the sector works closely with government, regulators, law enforcement and other industries to prevent harm, disrupt criminals and bring offenders to justice.

The industry response is being delivered through a broad and coordinated programme of activity:

Activity	Achievements
<p>Dedicated Card and Payment Crime Unit (DCPCU) – an industry-funded, fully operational police unit with a national remit, formed through collaboration between UK Finance, the City of London Police and the Metropolitan Police Service. The DCPCU investigates, targets and, where appropriate, arrests and supports the prosecution of offenders responsible for fraud affecting the payments, banking and finance industry.</p>	<p>Since 2004, the unit has prevented just over £1 billion from being stolen from customers, disrupted 421 organised crime groups, made 2,445 arrests, secured 1,110 convictions and recovered more than 2.6 million customer card or account details, or cheques. These outcomes demonstrate the operational value of sustained, specialist enforcement capability.</p> <p>In 2025 alone, the unit saved the sector and its customers £273 million, up from £64.9 million in 2024. It also disrupted 157 serious and organised criminals reinforcing its importance as a frontline defence against organised fraud.</p> <p>Operation Henhouse</p> <p>As part of this nationwide fraud intensification operation, the DCPCU helped deliver 31 arrests. Seizures included 50 devices, £13,000 in cash, c. £10,000 of counterfeit goods, an estimated £20,000 in listed assets, and £20,000 of equipment used to facilitate fraud. In addition, nearly £600,000 was made subject to account freezing orders. In two cases, DCPCU officers undertook operational activity targeting individuals and organised crime groups previously involved in serious and violent crime who have now been charged with fraud.</p> <p>Protect</p> <p>The unit also works closely with industry partners to protect customers from fraud and cybercrime, including by educating financial institution staff and customers. In 2025, the DCPCU delivered 118 training presentations to 8,605 individuals.</p> <p>The DCPCU took part in a nationwide fraud intensification operation, which measured suspect interventions, warrants executed, organised crime disruptions and assets seized. As of March the results of this collaboration were: 22 arrests, 13 warrants and £258,398 worth of assets and cash seized. In two of the cases DCPCU officers undertook operational activity targeting individuals and organised crime group's (OCG) who had previously been involved in serious and violent crime and have now been charged with committing fraud.</p>

Activity	Achievements
Intelligence Unit – a dedicated unit within UK Finance that enables intelligence sharing between members and law enforcement on emerging threats, data breaches and compromised card details.	<p>In 2025, the Intelligence Unit repatriated 2,774,022 compromised card numbers, enabling card issuers to act quickly to protect customers and prevent money from being stolen.</p> <p>Members shared more than 929,000 intelligence records, generating associated savings of £4.9 million, which were shared with law enforcement. Data collected by the unit also showed that 12,438 money mules were disrupted in 2025, underlining the value of timely intelligence sharing in identifying threats and preventing criminal exploitation.</p>
The Banking Protocol rapid response scheme – an initiative launched by UK Finance, National Trading Standards and local police forces that trains bank, building society, Post Office and credit union branch teams to identify warning signs that a customer may have been targeted by a criminal, and to alert local police so they can intervene and investigate.	<p>Since its inception, the scheme has led to more than 81,000 emergency calls to police, 1,662 arrests and the prevention of £433 million being stolen from customers, demonstrating the power of rapid intervention at the point of risk.</p> <p>In 2025, the scheme prevented £58.8 million from being stolen from customers and led to 12,034 emergency calls and 136 arrests, showing that coordinated local action continues to deliver tangible results for customers and law enforcement alike.</p> <p>Case study: Banking Protocol</p> <p>In April 2025, a Banking Protocol call was made by a staff member at a high street bank branch about two customers who had recently paid a roofing company £16,000 for guttering work and had returned to the branch after being asked for a further £15,000. The roofers had followed the customers to the bank in their van and were waiting outside. Officers were dispatched, stopped the van and arrested the two occupants on suspicion of fraud. The customers, who were identified as vulnerable, said they had been cold-called by the company, which they described as very pushy. Payments had already been taken via a chip-and-PIN machine, and no contract had been provided. The intervention prevented further crime.</p>
Vulnerable Victims Notification – a UK Finance and law enforcement initiative that enables local police forces to notify payment service providers (PSPs) of customer vulnerabilities that may make them more susceptible to fraud.	<p>In 2025, PSPs received 741 notifications from law enforcement regarding customer fraud vulnerabilities. Twenty-seven banking brands participate, and nearly two thirds of police forces (32 of 45) now use the process. All figures are higher than in 2024, reflecting stronger adoption of a practical tool for protecting customers at heightened risk.</p>
Cross-sector collaboration – ongoing work with other sectors, including telecoms and technology companies, as well as regulators such as Ofcom, to drive data-sharing and intelligence activity that mitigates live scam threats and supports effective regulation.	<p>Advert screening: UK Finance collaborated with a major platform to test whether shared intelligence could improve advert screening, resulting in a 30 per cent uplift in the detection of fraudulent adverts.</p> <p>Scams Signal: Real-time signals from mobile networks to banks demonstrating how valuable cross-sector data sharing can be in creating scalable mitigation solutions.</p> <p>Online Crime Centre: The industry is working with government to operationalise the Online Crime Centre, to support more effective public-private cross-sector data sharing at scale.</p>

Activity	Achievements
	<p>Investment firms and government agencies allowed list: Implementation of the registered investment firm list, along with a list for government agencies, is helping to reduce impersonation and investment scams.</p> <p>Industry learning sessions: Collaboration with leading technology firms is helping educate both members and technology partners on mobile device protection.</p> <p>Advocacy: Sustained advocacy for greater fraud accountability in the technology and telecoms sectors has included engagement with ministers, ambassadors to the UK, international trade associations, regulators, consumer groups and the media.</p>
<p>Customer education and awareness campaigns</p> <p>– UK Finance delivers year-round customer education through the Take Five to Stop Fraud campaign, helping people and businesses protect themselves from fraud. Its Don't Be Fooled campaign aims to inform people about the risks of sharing their bank details and deter them from becoming money mules.</p>	<p>The Take Five to Stop Fraud campaign gives the industry a strong, unified platform for delivering clear and consistent fraud prevention advice. With 38 major banks and building societies signed up, the campaign has significant reach and plays an important role in helping people protect their money and personal information.</p> <p>In 2025, this included:</p> <ul style="list-style-type: none"> • launching 'Match Ready' for Take Five Week 2025, encouraging people to strengthen their defences against fraud through a football-themed campaign and online quiz; • launching 'Protect Your Patch' in partnership with the National Allotment Society to provide advice and information for older audiences; • launching 'Type Don't Tap' to raise awareness of unauthorised card fraud and the importance of protecting personal information, one-time passcodes and online activity; • partnering with the BBC for BBC Scam Safe Week, including participation in a multi-platform programme and roadshow events across the UK; • delivering a year-round programme of social media activity to share fraud awareness advice on platforms with high dwell times. <p>The Don't Be Fooled schools programme, which holds the Young Enterprise Quality Mark, has educated more than 33,000 pupils at 470 schools about the risks of becoming a money mule. The campaign has also equipped law enforcement officers with a dedicated school engagement toolkit and expanded its reach through a refreshed website and new social media channels, including the Quick and Easy Money campaign targeting students and parents.</p>

BioCatch/Nasdaq Verafin

Foreword

Fraud at an Inflection Point: The Need for Collaboration

Once a crime of opportunity, fraud is now a global industry, surpassing the Gross Domestic Product (GDP) of most countries. Organised criminal networks run compounds staffed by trafficking victims and use Artificial Intelligence (AI) to hone, personalise, and automate cross-border attacks. Increasingly, these attacks target human behaviour to bypass bank controls.

Nasdaq Verafin's 2026 Global Financial Crime Report highlights the scale of the issue. Global consumers lost an estimated £430 billion to fraud in 2025, an annual rise of 9.2 per cent since 2023.

Fraud's impact extends beyond fiscal harm, eroding institutional trust, weakening economic resilience, and threatening national security. Reducing losses meaningfully, in the UK and globally, requires a fundamental shift. Only greater collaboration across institutions, sectors, regulators, and law enforcement will turn the tide. This shift must move from reactive detection to proactive prevention.

In the UK, fraud remains the most prevalent crime, victimising millions each year. The consequences are both financial and deeply personal, ranging from life-altering losses to emotional distress and diminished confidence in financial systems and communities. Often linked to organised crime and exploitation, fraud must be treated as a societal as well as an economic issue.

The UK Government's Fraud Strategy 2026-2029 recognises fraud as a national priority

and notes that no single organisation can address it alone. All stakeholders are urged to share information, align efforts, and participate in initiatives to achieve effective prevention and mitigation.

Mandatory reimbursement for APP fraud is fundamentally reshaping incentives across the payment ecosystem. Payment Service Providers of all sizes must shift toward fraud prevention that stops APP fraud before funds move, denying criminals the opportunity to profit from it.

Criminals' innovation frequently outpaces that of the sector. BioCatch data from nine UK financial institutions shows a 62 per cent spike in scam attempts in 2025 across over one hundred million accounts. The spike is due to more social engineering schemes. Purchase, investment, and romance scams have risen sharply, indicating greater manipulation by scammers. Phishing attempts are up 140 per cent; fraud with stolen devices rose 112 per cent last year. Attackers now blend digital and physical tactics. Reported mule activity increased by 16 per cent, indicating organised money laundering.

Traditional fraud methods, such as remote access and malware, have declined. This does not mean reduced risk. Instead, it shows how criminals now exploit human behaviour rather than technical flaws.

Criminals use AI to scale and refine attacks, crafting convincing impersonation scams

and deploying deepfakes during account openings. Synthetic identities and “selfie injections” let fraudsters bypass ID checks. These advances lower barriers, boost success, and allow rapid scaling, especially with agentic AI, which is likely the next force multiplier for global criminals.

As the landscape grows more complex, the same technologies that enable fraud also present opportunities to combat it. This highlights the dual role of advanced technology in today’s fraud environment.

Advances in AI and analytics let financial institutions move beyond static controls and implement dynamic, real-time risk assessments to identify and stop social engineering scams.

Behavioural intelligence shows not just what users do, but how. It finds subtle anomalies in user patterns, even with valid credentials. Consortium datasets provide a broader view of criminal risk, connecting transactions, accounts, and entities to enable deeper insights and earlier fraud detection. Combining behavioural and consortium intelligence helps institutions see risk holistically and take more proactive action.

The 2026 Fraud Report shows UK fraud losses are rising. However, prevented losses are outpacing criminal gains, forcing fraudsters to work harder for past results. Even the most advanced technologies alone are not enough. Human and organisational collaboration remains essential for an effective response.

Fraud is a shared challenge requiring a shared solution. Act today: Leverage consortium intelligence, commit to responsible data sharing, and collaborate across the industry to outpace criminals and reduce losses.

UK Finance calls on the financial ecosystem to unite in active information sharing and joint anti-fraud initiatives. We echo this,

stressing that cross-border collaboration and continuous sector alignment are essential to meaningful fraud reduction.

Fighting fraud is more than protecting assets. It is about protecting people. Every case represents a real person losing money, suffering psychological strain, and losing trust in institutions and digital platforms. As fraud becomes more targeted, action is urgent. Prevention is a societal duty.

Fraud is at a turning point. The industry’s response must now centre on collaboration, innovation, and shared responsibility. This is pivotal for addressing new challenges and making real progress.

UK leaders should harness data, leverage technology, and foster cross-border collaboration now to reduce harm, strengthen trust, and decisively turn the tide against criminals who stole £1.28 billion from UK bank accounts last year.

Jonathan Frost

Director,
Global Advisory



Kamlesh Harry,

Principal Strategic Advisor,
Fraud & Financial Crime



01

UK Finance Insight

£1.28B^{+4%}

stolen through fraud in 2025

4.06M^{+11%}

confirmed cases in 2025

£1.68B^{+11%}

of unauthorised fraud prevented by industry in 2025,

Unauthorised fraud

In an unauthorised fraudulent transaction, the account holder themselves does not provide authorisation for the payment to proceed, and the transaction is carried out by a third-party.

Authorised fraud

In an authorised fraudulent transaction, the account holder themselves is tricked into sending money to a fraudster posing as a genuine payee.

Losses

Total value of gross losses (unauthorised and authorised)

	2020	2021	2022	2023	2024	2025	Change
Unauthorised	£783.8m	£730.4m	£726.9m	£708.7m	£744.2m	£703.4m	-5%
Authorised	£420.7m	£583.2m	£485.2m	£459.7m	£484.0m	£576.4m	19%
Total	£1,204.6m	£1,313.6m	£1,212.1m	£1,168.4m	£1,228.2m	£1,279.8m	4%

Cases

Total number of confirmed cases (where a loss has occurred)

	2020	2021	2022	2023	2024	2025	Change
Unauthorised	2,910,509	2,912,467	2,781,311	2,729,807	3,444,481	3,814,128	11%
Authorised	154,614	195,996	207,372	232,427	231,474	248,070	7%
Total	3,065,123	3,108,463	2,988,683	2,967,363	3,675,955	4,062,198	11%

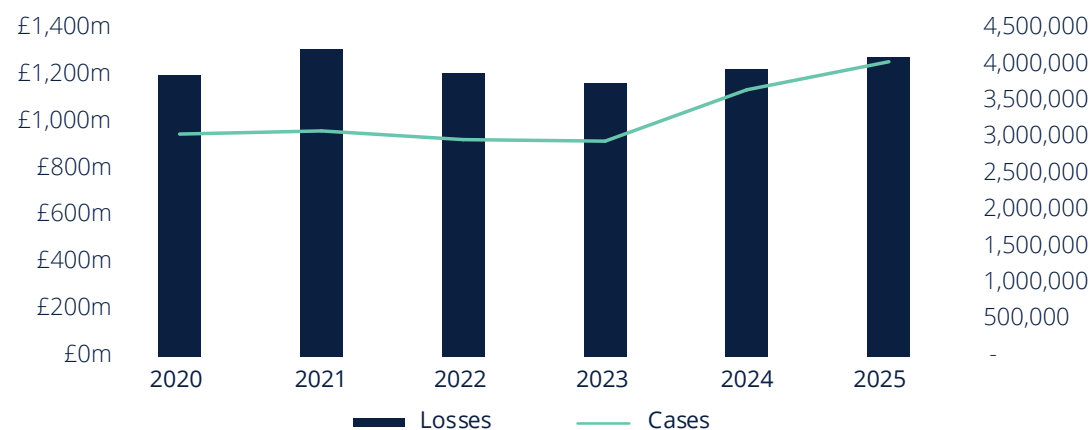
*Comparable data not available for authorised fraud prior to 2020

UK Finance's comprehensive industry data on the scale of fraud continues to highlight unrelenting attack levels from criminals in 2025. Both the total number of fraud cases reported to UK Finance members and the value of money lost to fraud recorded the second consecutive year of growth.

Last year's increase took the number of cases across both authorised and unauthorised fraud to a new record high of nearly 4.1 million, while losses, at £1.28 billion, were the highest since the peak during the pandemic in 2021 (**chart 1**). This represents year-on-year increases of 11 per cent and four per cent, respectively.

The efforts of the banking and payments industry to detect and prevent fraud continue to try and keep pace with the persistent threat from criminals. In 2025 70p of every £1 of unauthorised fraud attempted was prevented without a loss occurring. This equated to £1.68 billion of prevented fraud. The 11 per cent increase in the value of fraud that was stopped provides further indication of the rise in attack levels against individuals and institutions.

Chart 1: Number of fraud cases and value of losses



Source: UK Finance

The overall picture is one of escalating challenge for the banking and payments industry in ensuring investment in systems and infrastructure is responding to the evolving tactics of fraudsters. It also reinforces the need for individuals to keep personal data secure and be continually vigilant about scammers' evolving tactics. Furthermore, this needs to be underpinned with similar efforts from channels that criminals use to enable fraudulent activity, such as social media and telecoms firms, to close down the routes used to initiate fraud.

The need for this whole system approach is clear when we look at the evolution of different types of fraud over the past year. Our data shows a material increase in the number of both unauthorised and authorised payment (APP) fraud cases (11 per cent and seven per cent respectively). However, the increase in fraud losses in 2025 was entirely driven by an increase in APP fraud – a 19 per cent increase on 2024, while unauthorised losses resumed a downward trend in 2025.

Our data sees two distinct trends in play in 2025, the beginnings of which we observed in our 2025 Half-Year Fraud Report. Attack levels on cards, in particular, posted a significant increase last year, but criminals are targeting many more individuals to secure the same

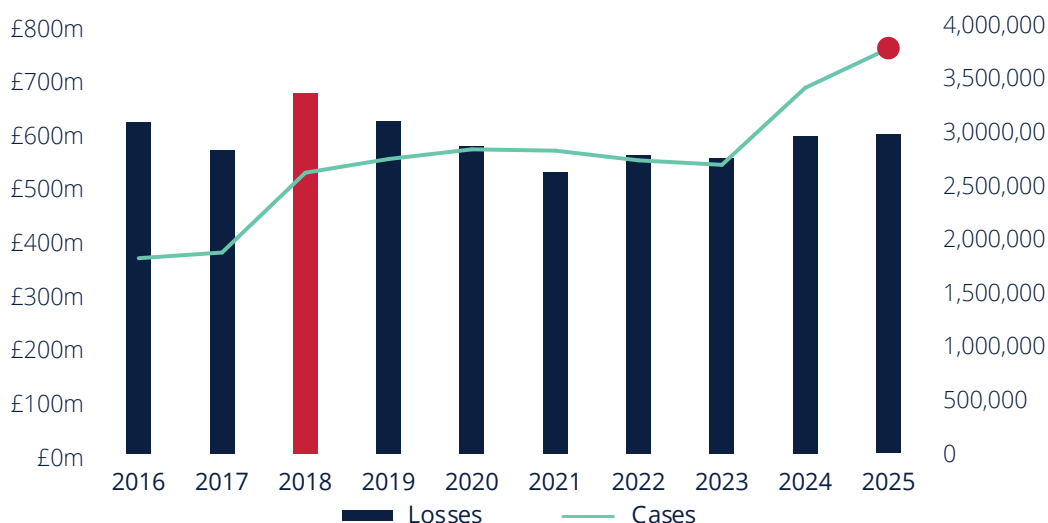
loss – a clear move towards a higher volume, lower value trade off. The reverse is true for authorised payment fraud, with the more prevalent MO shifting towards convincing victims to transfer higher sums of money to what they believe are legitimate sources or opportunities. We will look at how our data breaks down against these trends in more detail.

1. High volume, low value

Of the 4.1 million total cases recorded in 2025, 3.8 million of these were categorised as unauthorised – an 11 per cent increase on 2024 and a series high. Despite the significant growth in case numbers in 2025, the total value of unauthorised losses fell five per cent compared with the previous year.

The vast majority of unauthorised cases (99%) occur on debit and credit cards. **Chart 2** provides a stark illustration of the shift to a much larger number of lower value cases. 2025 saw an 11 per cent increase in card fraud case volumes, while losses were broadly unchanged from the previous year. The peak year for losses was 2018 but, while 2025 saw losses 11 per cent *lower* than the high-water mark, case numbers are 44 per cent *higher*.

Chart 2: Number of card fraud cases and value of losses

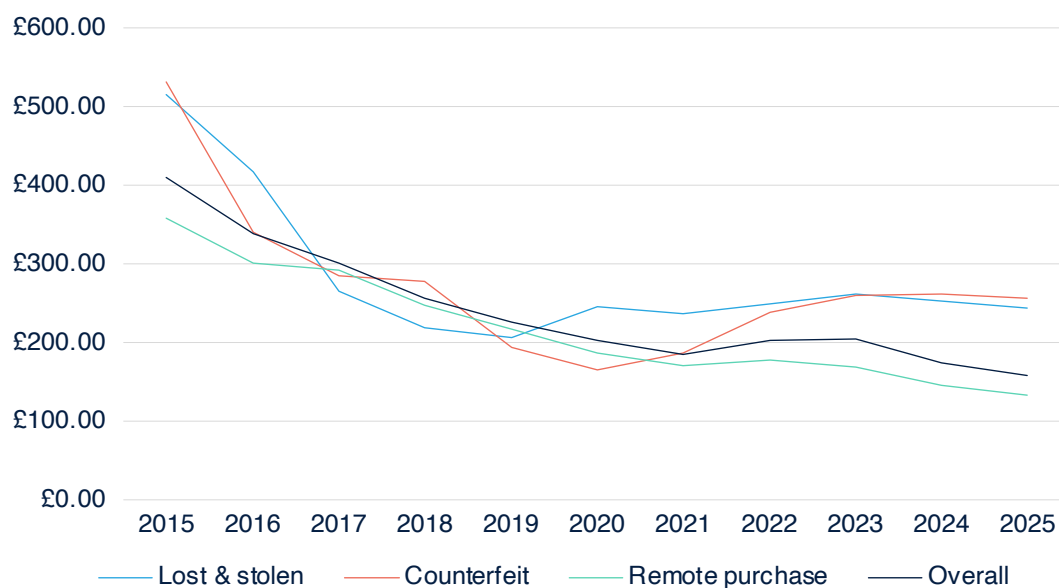


Source: UK Finance

A significant contributor to the surge in card fraud case has been remote purchase (also known as card not present or CNP) fraud. This fraud occurs when a criminal uses stolen card details to buy something on the internet, over the phone or through mail order. We noted the beginning of this trend in last year's fraud report, and 2025 saw a further 13 per cent increase in the number of remote purchase fraud cases with a total value of £423.5 million (a three per cent increase on 2024). Remote purchase (CNP) fraud case volumes now total more than all fraud categories combined for any year prior to 2024.

As we also noted in last year's report, intelligence continues to point to social engineering to extract one-time passcodes (OTPs for example), which are then used to register digital wallets or make one-off transactions, as a prevalent means of compromising credit and debit cards. While the introduction of secure customer authentication and OTPs has introduced additional friction for fraudsters, these measures are nevertheless being bypassed by criminals through social engineering. They have, however, driven down the average loss incurred per case (see **chart 3**).

Chart 3: Average case value by card fraud type



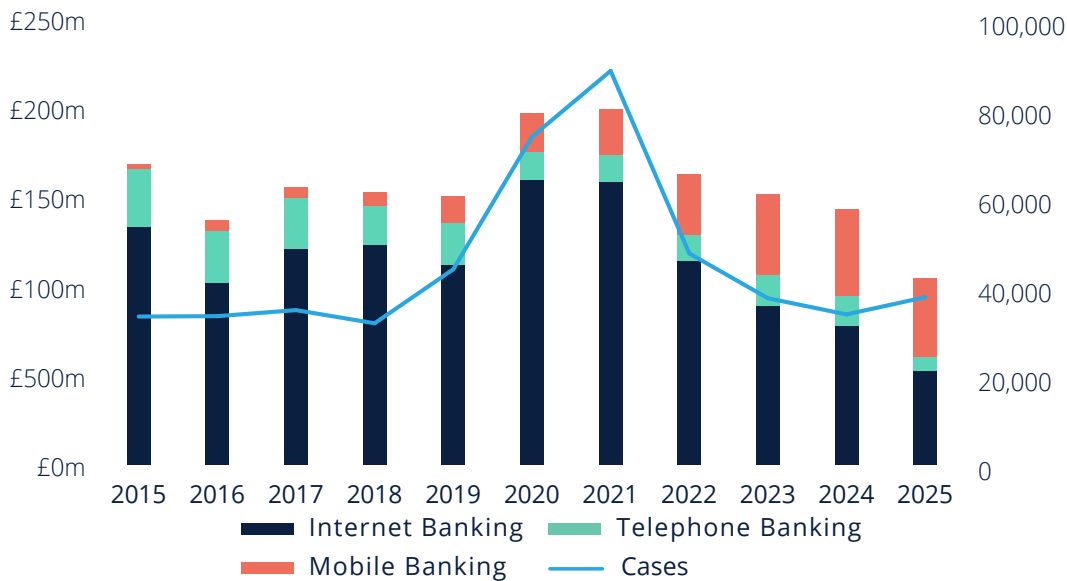
Source: UK Finance

In 2015, the average loss per case across all card fraud types was £410. In 2025, this had fallen to £158. And in remote purchase cases, average case values have dropped by nearly three-fifths in the past decade from £300 to £132. While on the surface this may appear to be a better outcome for

customers, it still represents significant sums ending up in the hands of criminals as well as significantly more people having to deal with the hassle, administration, and emotional toll of reporting or cancelling cards, even though almost all cases will be refunded by their bank.

The other component of unauthorised fraud is via remote banking channels. 2025 trends across combined online, telephone, and mobile banking are similar to that seen across cards. The number of cases across the three channels rose by 11 per cent, but losses were 27 per cent lower than in 2024 (**chart 4**).

Chart 4: Number of remote banking cases and losses



Source: UK Finance

Delving into trends in each of the channels, trends in fraudulent activity more closely mirror changes in usage. The main area of growth continues to be in mobile banking. In 2025, we observed the highest number of cases ever recorded (just over 25,000); a 21 per cent increase on 2024. This continues to track growth in registrations and usage. UK Finance's forthcoming UK Payment Markets report will show another year of strong growth in regular mobile banking users, following growth of more than a quarter in 2024.

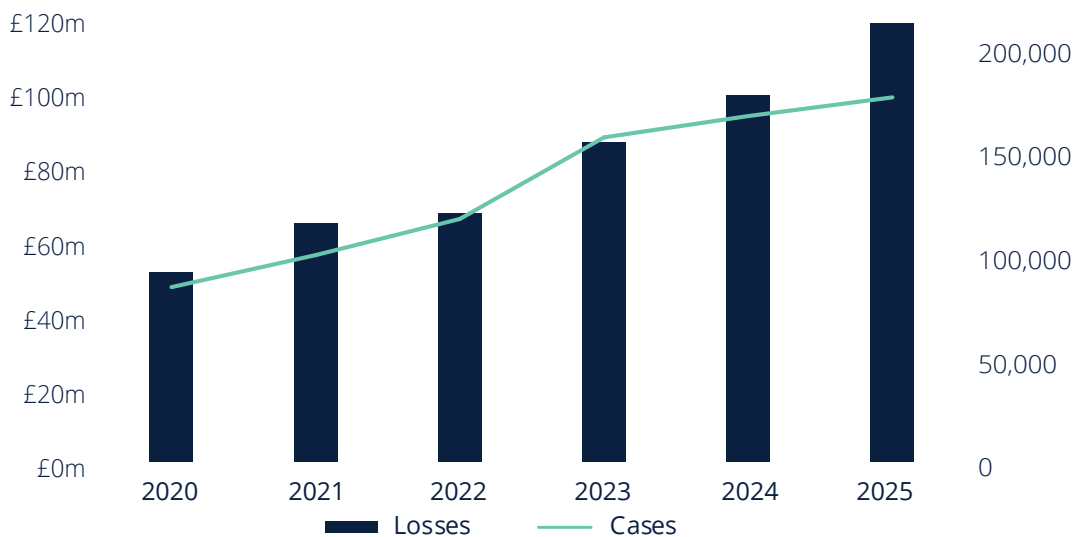
Similar to that reported on cards, mobile banking losses fell by ten per cent. The resulting reduction in average loss per case to the lowest since 2016 again reflects consumer behaviour, e.g. using mobile banking to transfer smaller amounts of money, as well as ongoing security enhancements to mobile banking services.

Prevention rates across all remote banking channels increased overall in 2025, to 70 per cent from 65 per cent in the previous year. Elsewhere in remote banking, losses across online and telephone channels continued to head lower. Losses via online banking were the lowest since 2011 and for telephone banking, the lowest ever reported.

2. The rise and rise of malicious payees

The second notable trend in our 2025 fraud data relates to authorised payment fraud. Across the whole category of APP fraud, our data reports a significant 19 per cent increase in losses, to £576.4 million, in 2025. At the same time the number of cases rose by seven per cent – the highest for which comparable data are available.

Chart 5: Number of authorised fraud cases and losses



Source: UK Finance

UK Finance members report APP fraud across eight different scam types, and there are some distinct movements underneath the total (**chart 5**). In some scam types we have seen a steady, and in some cases sizeable, decline in cases and losses post-pandemic. These can be grouped together under the banner of malicious redirection – an individual intends to make a payment to a legitimate payee, but the funds are redirected to a third party. An example of this can include an individual intending to send funds for a house purchase deposit to their solicitor but instead receiving instructions from a criminal third party with new account details.

In each of the four categories that make up malicious redirection fraud; invoice & mandate, CEO, impersonation: police/bank, and impersonation: other, our data shows year-on-year losses in three of the categories to the lowest since 2020 (**table a**).

And collectively, these scam types now account for just under a quarter of all APP losses, down from over half in 2020 (case volumes have fallen to 11 per cent from 30 per cent over the same period).

Malicious Redirection

DEFINITION: A payer intends to pay a legitimate payee but, as a result of a scam, instead pays a malicious third party due to the actions of that third party.

Comprised of 4 scam types – Invoice & Mandate, CEO, Impersonation: Police / Bank Staff and Impersonation: Other

Malicious Payee

DEFINITION: A payer may pay funds to a correctly identified payee for what they believe are legitimate purposes but then becomes victim to a scam e.g. payee absconds with the funds without providing goods or services. Authorised, correctly-directed, payments that are disputed under these circumstances are referred to as malicious payees.

Comprised of 4 scam types – Purchase, Investment, Romance and Advance fee

Table A: Losses by Fraud type

Malicious Redirection		
Invoice and Mandate	↓	£41.3m Lowest since 2020
CEO	↓	£5.6m Lowest since 2021
Impersonation: Bank/Police	↓	£55.5m Lowest since 2020
Impersonation: Other	↓	£36.9m Lowest since 2020

Malicious Payee		
Purchase	↑	£118.1m Highest ever
Investment	↑	£221.5m Highest ever
Romance	↑	£39.2m Highest ever
Advance fee	↑	£58.4m Highest ever

In contrast the APP growth industry is malicious payee fraud. Scam types under this banner typically involve an individual believing a transaction is for legitimate goods or services, which are ultimately not provided. The most common malicious payee fraud type is investment scams. Purchase scams, romance fraud and advance fee fraud are also forms of malicious payee fraud.

Each of these scam types saw the highest level of losses recorded in 2025 and combined saw a 35 per cent increase in reported losses (£437 million) compared with 2024.

It is, however, important to note that some of the malicious payee scam types have a long gestation period. Our data captures the loss at the point at which the fraud has been

confirmed. As it can take time, sometimes years, before individuals realise they have been victim of an investment or romance scam and then report it, many of the cases logged in 2025 are likely to have been initiated some time prior to that.

This alone does not account for the rapid rise in these fraud types in the past year. The characteristics of malicious payee fraud and the tools available to the banking and payments industry to stop it are different from those used to combat malicious redirection scams. For example, in the case of the latter, confirmation of payee and warning messages during the payment journey may help to capture fraudulent transactions earlier in the process.

Whereas, in the case of an investment scam, if individuals believe the payee is who they say they are, they are likely to proceed with a payment regardless of warnings. Moreover, these scams often start with smaller value payments, which may not appear unusual and are therefore more difficult to detect as subsequent transaction values increase.

Malicious payee fraud is not just a growth industry; it is a global one. From Canada to Malaysia, banks and law enforcement are focused on raising awareness of the growing scourge of investment scams, in particular.

There is no let up in the fight against fraud. The sums of money ending up in the hands of criminals each year, just from the UK, are growing and the number of victims is growing faster still. In 2025, the banking and payments industry also succeeded in blocking even greater amounts going to fraudsters.

The financial sector has introduced more hurdles in the payments process for fraudsters, but without creating friction for consumers. It invests in sophisticated detection software, security measures on online platforms, and customer awareness campaigns. And it reimburses victims when criminals succeed. However, as our fraud data shows again this year the scale of attack from criminals is unrelenting and that requires a whole ecosystem approach to turn the tide.

02

Unauthorised Fraud Summary

Unauthorised fraud includes fraud on credit, debit and other payment cards, cheques and remote banking channels.

- Unauthorised fraud losses were **£703.4 million** in 2025, a decrease of 5% from 2024
- There were **3.81 million** confirmed cases of unauthorised fraud reported in 2025, an 11% increase on the total reported in 2024.
- The industry prevented a further **£1.68 billion** of unauthorised fraud – equivalent to 70p in every £1 of attempted fraud being stopped without a loss occurring.

Cards

Prevented: **£1.33bn** (+12%)
Losses: **£594.9m** (0%)
Cases: **3.78m** (+11%)

Cheques

Prevented: **£107.4m** (+100%)
Losses: **£4.1m** (-49%)
Cases: **795** (-28%)

Remote Banking

Prevented: **£240.2m** (-10%)
Losses: **£104.4m** (-27%)
Cases: **37,646** (+11%)

03

Unauthorised Card Fraud

Credit, Debit and other payment cards

This section covers all types of unauthorised card losses. Fraud losses on UK-issued cards totalled £594.9 million in 2025, a very slight increase from £592.5 million in 2024.

Losses

Total value of gross losses

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Change
Prevented	£986.0m	£984.8m	£1,126.4m	£1,007.5m	£983.4m	£966.6m	£974.2m	£1,021.6m	£1,190.6m	£1,333.3m	12%
Lost & stolen	£96.3m	£92.9m	£95.1m	£94.8m	£78.9m	£77.2m	£100.2m	£104.0m	£111.7m	£109.8m	-2%
CNR	£12.5m	£10.2m	£6.3m	£5.2m	£4.4m	£3.9m	£4.0m	£3.0m	£3.0m	£2.8m	-4%
Counterfeit	£36.9m	£24.2m	£16.3m	£12.8m	£8.7m	£4.7m	£4.7m	£4.7m	£3.9m	£4.7m	21%
CNP	£432.3m	£408.4m	£506.4m	£470.2m	£452.6m	£412.5m	£395.7m	£360.5m	£412.5m	£423.5m	3%
Card ID Theft	£40.0m	£29.8m	£47.3m	£37.7m	£29.7m	£26.3m	£51.7m	£79.1m	£61.5m	£54.0m	-12%
Total	£618.1m	£565.4m	£671.4m	£620.6m	£574.2m	£524.5m	£556.3m	£551.3m	£592.5m	£594.9m	0%
UK	£417.9m	£407.5m	£496.6m	£449.9m	£414.5m	£384.0m	£416.2m	£416.8m	£429.5m	£445.1m	4%
International	£200.1m	£158.0m	£174.8m	£170.7m	£159.7m	£140.5m	£140.1m	£134.5m	£163.1m	£149.8m	-8%

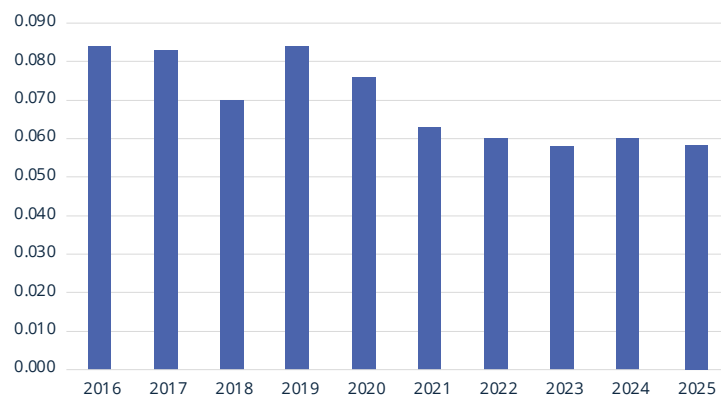
Cases

Total number of confirmed cases (where a loss has occurred). Figures relate to the total number of cards defrauded and not the number of individual customers.

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Change
Lost & stolen	231,164	350,279	434,991	460,142	321,994	325,501	401,340	397,549	441,582	449,189	2%
CNR	11,377	10,903	10,046	7,907	8,435	8,941	8,848	5,933	7,398	7,888	7%
Counterfeit	108,597	85,025	58,636	65,907	52,782	24,908	19,594	18,070	14,988	18,477	23%
CNP	1,437,832	1,398,153	2,050,275	2,157,418	2,417,866	2,425,099	2,221,026	2,127,201	2,830,293	3,196,962	13%
Card ID Theft	31,756	29,156	63,791	54,165	34,545	38,753	82,064	142,445	115,326	103,171	-11%
Total	1,820,726	1,873,516	2,617,739	2,745,539	2,835,622	2,823,202	2,732,872	2,691,198	3,409,587	3,775,687	11%

Fraud to turnover ratio

Year	Ratio	Change
2016	0.084	12%
2017	0.083	-1%
2018	0.070	-16%
2019	0.084	20%
2020	0.076	-10%
2021	0.063	-18%
2022	0.060	-5%
2023	0.058	-3%
2024	0.060	3%
2025	0.057	-5%



04

Analysis by Unauthorised Card Fraud Case Type

Lost and Stolen Card Fraud

Value = £109.8m (-2%)**Cases = 449,189 (2%)**

This fraud occurs when a criminal uses a lost or stolen card to make a purchase or payment (whether remotely or face to face) or takes money out at an ATM or in a branch. Typically, this involves obtaining cards through low tech methods such as distraction thefts and entrapment devices attached to ATMs.

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Change
Value	£96.3m	£92.9m	£95.1m	£94.8m	£78.9m	£77.2m	£100.2m	£104.0m	£111.7m	£109.8m	-2%
Cases	231,164	350,279	434,991	460,142	321,994	325,501	401,340	397,549	441,582	449,189	2%

Key Stats / Insights

- Highest case total reported since 2019
- There are five per cent more cards in issue in 2025 than in 2023; more cards in issue will result in more opportunities for a card to be lost or stolen so rises are to be expected.

Card not received

Value = £2.8m (-4%)

Cases = 7,888 (7%)

This type of fraud occurs when a card is stolen in transit, after a card issuer sends it out and before the genuine cardholder receives it.

Criminals typically target properties with communal letterboxes such as flats, student halls of residence and external mailboxes to commit this type of fraud. People who do not get their mail redirected when they change address are also vulnerable to this type of fraud.

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Change
Value	£12.5m	£10.2m	£6.3m	£5.2m	£4.4m	£3.9m	£4.0m	£3.0m	£3.0m	£2.8m	-4%
Cases	11,377	10,903	10,046	7,907	8,435	8,941	8,848	5,933	7,398	7,888	7%

Key Stats / Insights

- More cards in issue means that more cards need to be sent to customers which results in greater opportunities for them to be intercepted. However, case numbers this year are below the average for the past decade. In addition, banks are now starting to issue cards with longer expiry dates which means fewer cards will need to be reissued in the longer term. This should result in a reduction in this type of fraud.

Counterfeit Card Fraud

Value = £4.7m (21%)

Cases = 18,477 (23%)

This fraud occurs when a criminal creates a fake card using information obtained from the magnetic stripe.

To obtain the data required to create a counterfeit card, criminals attach concealed or disguised devices to the card-reader slots of ATMs and unattended payment terminals (UPTs), such as self-service ticket machines at railway stations, cinemas, and car parks. The counterfeit cards are typically used overseas in countries yet to upgrade to chip and PIN.

The continuous decrease in this type of fraud since 2008 is a result of the introduction of chip technology in the UK and its subsequent increased adoption around the world which has restricted fraudsters use of the counterfeit cards

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Change
Value	£36.9m	£24.2m	£16.3m	£12.8m	£8.7m	£4.7m	£4.7m	£4.7m	£3.9m	£4.7m	21%
Cases	108,597	85,025	58,636	65,907	52,782	24,908	19,594	18,070	14,988	18,477	23%

Key Stats / Insights

- Cards continue to be used in regions without chip and PIN technology.
- Whilst an increase on last year has been reported, losses in this category remain consistent with post-Covid trends.

Remote Purchase Fraud (CNP)

Value = £423.5m (3%)

Cases = 3,196,962 (13%)

This fraud occurs when a criminal uses stolen card details to buy something on the internet, over the phone or via mail order. It is also referred to as card not present (CNP) fraud.

Feedback suggests that criminals are using increasingly sophisticated social engineering techniques to trick customers into divulging their OTPs amongst other tactics so they can authenticate fraudulent online card transactions. Criminals are also taking advantage of the increasing tendency for online shoppers to search for discounted items on social media. When a customer goes to buy the product advertised on a 'fake' social media profile, the criminal uses stolen card details to purchase the item from a legitimate source and then keeps the payment from the customer.

Industry-supported information and awareness campaigns on how consumers can protect themselves online, and ensuring OTPs remain secure are important tools in the fight against this type of fraud.

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Change
Value	£432.3m	£408.4m	£506.4m	£470.2m	£452.6m	£412.5m	£395.7m	£360.5m	£412.5m	£423.5m	3%
Cases	1,437,832	1,398,153	2,050,275	2,157,418	2,417,866	2,425,099	2,221,026	2,127,201	2,830,293	3,196,962	13%

Key Stats / Insights

- Highest loss total reported since 2020.
- Highest case total ever reported and more cases than all fraud categories combined for any year other than 2024.
- Criminals continue to socially engineer victims into disclosing OTPs which are then being used to register for digital wallets or undertake one off transactions online.
- Average case values have fallen from £300 in 2016 to £132 in 2025; a 56% reduction.

Card ID Theft

Value = £54.0m (-12%)

Cases = 103,171 (-11%)

Card ID theft occurs when a criminal uses a fraudulently obtained card or card details, along with stolen personal information, to open or take over a card account held in someone else's name.

This type of fraud is split into two categories: third-party application fraud and account takeover fraud.

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Change
Value	£40.0m	£29.8m	£47.3m	£37.7m	£29.7m	£26.3m	£51.7m	£79.1m	£61.5m	£54.0m	-12%
Cases	31,756	29,156	63,791	54,165	34,545	38,753	82,064	142,445	115,326	103,171	-11%

Third Party Application:

Value = £16.1m (-17%)

Cases = 21,141 (-13%)

With third-party application fraud, a criminal will use stolen or fake documents to open a card account in someone else's name. This information will typically have been gathered through data loss, such as via data hacks and social engineering to compromise personal data.

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Change
Value	£15.6m	£11.3m	£29.4m	£17.4m	£15.1m	£10.9m	£17.3m	£31.8m	£19.5m	£16.1m	-17%
Cases	10,958	8,359	28,203	18,953	12,940	16,183	16,687	20,795	24,407	21,141	-13%

Account Takeover:

Value = £37.8m (-10%)

Cases = 82,030 (-10%)

In an account takeover fraud, a criminal takes over another person's genuine card account.

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Change
Value	£24.4m	£18.4m	£17.9m	£20.3m	£14.6m	£15.4m	£34.5m	£47.4m	£42.0m	£37.8m	-10%
Cases	20,798	20,797	35,588	35,212	21,605	22,570	65,377	121,650	90,919	82,030	-10%

Key Stats / Insights

- Second consecutive year of decrease for Card ID theft after the peak reported in 2023. Losses in 2025 have fallen 32% in comparison to 2023 whilst cases have fallen 28%.

05

Further Card Fraud Analysis

Note: Figures in the following sections relate to the places where the card was used fraudulently, rather than how the card or the card details were compromised. This is simply another way of breaking down the overall card fraud totals and so these figures should not be treated as an addition to those already covered in the earlier sections. Case volumes are not available for the place of misuse, as it is feasible that one case could cover multiple places, e.g. a lost or stolen card could be used to make an ATM withdrawal as well as to purchase goods on the high street.

UK Retail Face to Face Fraud

Value = £86.3m (1%)

UK retail face-to-face card fraud covers all transactions that occur in person in a UK shop, including contactless. Much of this fraud is undertaken using low-tech techniques, with fraudsters finding ways of stealing the card, and often the PIN, to carry out fraudulent transactions in shops.

This includes criminals using methods such as ATM card entrapment and distraction thefts, combined with shoulder surfing and PIN pad cameras. Criminals also use various social engineering methods to dupe victims into handing over their cards on their own front doorstep, often known as courier scams.

This category includes fraud incidents involving the contactless functionality on both payment cards and mobile devices.

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Change
Value	£62.8m	£61.9m	£69.8m	£64.3m	£48.9m	£48.3m	£72.0m	£88.7m	£85.3m	£86.3m	1%

Key Stats / Insights

- Contactless fraud totalled £46.8m in 2025, an eight per cent increase on the total reported in 2024.

UK Internet / E-Commerce Card Fraud Losses

Value = £250.8m (9%)

These figures cover fraud losses on card transactions made online and are included within the overall remote purchase (card not present) fraud losses described in the previous section.

Data compromise, including through data hacks at third parties such as retailers, is a major driver of these fraud losses, with criminals using the stolen card details to make purchases online. The data stolen from a breach can be used for months or even years after the incident. Criminals also use the publicity around data breaches as an opportunity to trick people into revealing financial information.

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Change
Value	N/A	N/A	£254.4m	£232.6m	£242.8m	£236.1m	£220.5m	£202.4m	£230.9m	£250.8m	9%

*Data not available prior to 2018

Key Stats / Insights

- Highest total reported since 2018.

UK Cash Machine Fraud Losses

Value = £25.7m (0%)

These figures cover fraudulent transactions made at cash machines in the UK, either using a stolen card or where a card account has been taken over by the criminal. In all cases the fraudster would need to have access to the genuine PIN and card. Most losses result from distraction thefts which occur mainly in shops, bars and restaurants and at ATMs.

Fraudsters also target cash machines to compromise or steal cards or card details in three main ways:

Entrapment devices: Inserted into the card slot in a cash machine, these devices prevent the card from being returned to the cardholder. To capture the PIN, the criminal will use a small camera attached to the machine and directed at the PIN pad, or they will watch it being entered by the cardholder. Once the customer leaves the machine, the criminal removes the device and the card and subsequently uses it to withdraw cash.

Skimming devices: These devices are attached to the cash machine to record the details from the magnetic strip of a card, while a miniature camera captures the PIN being entered. A fake magnetic stripe card is then produced and used with the genuine PIN to withdraw cash at machines overseas which have yet to be upgraded to Chip and PIN.

Shoulder surfing: A technique used by criminals to obtain PINs by watching over the cardholder's shoulder when they are using an ATM or card machine. The criminal then steals the card using distraction techniques or pickpocketing.

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Change
Value	£43.1m	£37.2m	£32.6m	£30.0m	£28.1m	£24.4m	£26.1m	£25.6m	£25.8m	£25.7m	0%

UK / International Card Fraud

UK Value = £445.1m (4%)

INT Value = £149.7m (-8%)

These figures provide a breakdown of fraud committed on a UK-issued credit, debit, or charge card, split between whether the incident occurred in the UK or overseas.

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Change
UK	£417.9m	£407.5m	£496.6m	£449.9m	£414.5m	£384.0m	£416.2m	£416.8m	£429.5m	£445.1m	4%
International	£200.1m	£158.0m	£174.8m	£170.7m	£159.7m	£140.5m	£140.1m	£134.5m	£163.1m	£149.8m	-8%

06

Unauthorised Cheque Fraud

Value = £4.1m (-49%)

Cases = 795 (-28%)

There are three types of cheque fraud: counterfeit, forged and fraudulently altered.

Counterfeit

Value = £0.5m (-53%)

Cases = 139 (-49%)

Counterfeit cheques are printed on non-bank paper to look exactly like genuine cheques and are drawn by a fraudster on genuine accounts.

Fraudulently Altered Cheques

Value = £1.9m (-67%)

Cases = 292 (-50%)

A fraudulently altered cheque is a genuine cheque that has been made out by the customer but has been changed by a criminal before it is paid in, for example by altering the beneficiary's name or the amount of the cheque.

Forgery

Value = £1.7m (21%)

Cases = 364 (45%)

A forged cheque is a genuine cheque that has been stolen from an innocent customer and used by a fraudster with a forged signature.

All Cheque Fraud (2016-2025)

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	CHANGE
Prevented	£196.2m	£212.3m	£218.2m	£550.8m	£238.5m	£33.1m	£19.8m	£12.3m	£53.8m	£107.4m	100%
Value	£13.7m	£9.8m	£20.6m	£53.6m	£12.3m	£6.4m	£7.5m	£5.6m	£8.1m	£4.1m	-49%
Cases	3,388	1,745	2,020	2,852	1,247	815	966	1,197	1,106	795	-28%

Key Stats / Insights

- Lowest loss total ever reported.
- Lowest case total ever reported.
- Highest prevented value reported since 2020; 96% of all cheque fraud was prevented without any loss occurring.

07

Unauthorised Remote Banking Fraud

Value = £104.4m (-27%)

Cases = 37,646 (11%)

Remote banking fraud is organised into three categories: internet, telephone and mobile banking. It occurs when a criminal gains access to an individual's bank account through one of the three remote banking channels and makes an unauthorised transfer of money from the account.

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	CHANGE
Prevented	£205.4m	£261.1m	£317.7m	£268.9m	£393.8m	£365.5m	£174.1m	£218.1m	£265.4m	£240.2m	-10%
Value	£137.0m	£156.1m	£152.9m	£150.7m	£197.3m	£199.5m	£163.1m	£151.7m	£143.5m	£104.4m	-27%
Cases	33,392	34,746	31,797	43,920	73,640	88,450	47,473	37,412	33,788	37,646	11%

Key Stats / Insights

- Lowest loss total since 2014.
- £240.2m remote banking fraud was prevented without a loss occurring, equivalent to 70p in every £1.

The data included within the next three categories (Internet Banking, Telephone Banking and Mobile Banking) are a subset of Remote Banking and should not be treated as an addition.

Internet Banking Fraud

Value = £52.6m (-32%)

Cases = 9,562 (4%)

This type of fraud occurs when a fraudster gains access to a customer's bank account through internet banking using compromised personal details and passwords, and makes an unauthorised transfer of money.

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	CHANGE
Value	£101.8m	£121.2m	£123.0m	£111.8m	£159.7m	£158.3m	£114.1m	£88.7m	£77.8m	£52.6m	-32%
Cases	20,088	21,745	20,904	25,849	55,995	72,557	32,036	13,669	9,176	9,562	4%

Key Stats / Insights

- Reductions in fraud are to be expected as usage in this channel reduces.

Telephone Banking Fraud

Value = £7.9m (-53%)

Cases = 2,904 (-22%)

This type of fraud occurs when a criminal uses compromised bank account details to gain access to a customer's telephone banking account and makes an unauthorised transfer of money away from it.

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	CHANGE
Value	£29.6m	£28.4m	£22.0m	£23.6m	£16.1m	£15.5m	£14.7m	£17.6m	£16.7m	£7.9m	-53%
Cases	10,495	9,577	7,937	11,199	7,490	4,623	3,076	3,711	3,733	2,904	-22%

Key Stats / Insights

- Lowest loss total ever reported.
- Lowest case total ever reported.
- Voice biometric software continues to be an effective prevention tool in this channel, but declines are also reflective of declining use of telephone banking.

Mobile Banking Fraud

Value = £43.9m (-10%)

Cases = 25,180 (21%)

Mobile banking fraud occurs when a criminal uses compromised bank account details to gain access to a customer's bank account through a banking app downloaded to a device only.

It excludes web browser banking on a mobile and browser-based banking apps (incidents on those platforms are included in the internet banking fraud figures)

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	CHANGE
Value	£5.7m	£6.5m	£7.9m	£15.2m	£21.6m	£25.8m	£34.2m	£45.5m	£49.0m	£43.9m	-10%
Cases	2,809	3,424	2,956	6,872	10,155	11,270	12,361	20,032	20,879	25,180	21%

Key Stats / Insights

- Highest case total ever reported.
- First year on year reduction in losses ever reported.

08

Authorised Push Payment (APP) Fraud

Authorised Push Payment (APP) fraud occurs when a person is tricked into authorising a payment to a fraudster, where the recipient is not who the user intended to pay, or the purpose is fraudulent. It involves dishonest manipulation to persuade victims to transfer funds from their account.

		2020	2021	2022	2023	2024	2025	Change
Cases	Personal	145,207	188,964	200,643	224,692	224,857	240,566	7%
	Non-Personal	9,407	7,032	6,729	7,735	6,617	7,504	13%
	Total	154,614	195,996	207,372	232,427	231,474	248,070	7%
Payments	Personal	228,946	333,751	361,761	405,096	417,184	505,268	21%
	Non-Personal	15,625	11,386	10,505	12,364	10,995	14,165	29%
	Total	244,571	345,137	372,266	417,460	428,179	519,433	21%
Value	Personal	£347.4m	£505.9m	£408.2m	£376.4m	£399.0m	£500.8m	26%
	Non-Personal	£73.3m	£77.4m	£77.0m	£83.3m	£84.9m	£75.6m	-11%
	Total	£420.7m	£583.2m	£485.2m	£459.7m	£484.0m	£576.4m	19%
Returned to victim	Personal	£148.9m	£233.4m	£254.1m	£256.4m	£241.4m	£319.7m	32%
	Non-Personal	£25.8m	£24.3m	£31.5m	£30.8m	£30.3m	£34.6m	14%
	Total	£174.7m	£257.7m	£285.6m	£287.3m	£271.7m	£354.3m	30%

Cases: The number of confirmed cases reported, one case equals one account not one individual.

Payments: Total number of payments identified as fraudulent in relation to case reported above.

Value: The total value of payments reported above.

Returned to Victim: The total amount returned to the victim either through a direct refund from the victim's bank or through recovery of funds from the beneficiary account.

09

APP Fraud Enablers

Our annual reporting of fraud statistics draws information from banks and payment service providers on identified and reported fraudulent activity. It concentrates on the prevalence and nature of different fraud and scam types, as well as the losses incurred. This enables the industry and stakeholders to monitor change over time, informing ongoing detection and prevention strategies.

But most of the fraudulent activity starts outside the banking sector. Key to tackling and ultimately reducing losses and the impact on consumers is greater understanding on where and how fraud and scams originate.

UK Finance also publishes data on the source of authorised push payment fraud based on analysis of a subset of APP data which uses anonymised case data that includes insight on the reported enablers of fraud events.

This shows that:

- 66% of fraud cases are enabled by online sources. These cases tend to include lower-value scams such as purchase fraud and therefore account for 32% of total losses.
- 17% of fraud cases are enabled by telecommunications. These are usually higher value cases such as impersonation scams and so account for 28% of losses.

	2022		2023		2024		2025	
	Volume	Value	Volume	Value	Volume	Value	Volume	Value
Online	78%	36%	76%	30%	70%	29%	66%	32%
Telecommunications	18%	45%	16%	43%	16%	36%	17%	28%
Email	2%	12%	1%	11%	1%	10%	1%	7%
Other	1%	3%	2%	5%	3%	7%	5%	8%
Unable to ascertain	1%	4%	5%	11%	10%	18%	11%	24%

The Data:

- The Best Practice Standards (BPS) system is a secure platform which allows its members – which include, national and regional, domestic and international, physical and virtual, banks and non-banks, as well as payment service providers – to share information relating to fraud and ‘push payment’ scams.
- The BPS platform enables firms to create cases in real-time, quickly passing information to other financial institutions that have received fraudulent money. This greatly increases the chances of being able to freeze it and stop it ending up in a criminal’s hands.
- UK Finance has access to aggregate reporting from the BPS system, allowing it to assess the volume and value of fraud and scams and the origination of the fraudulent activity, as reported by the victim. Aggregate information is compiled only once members have investigated the fraudulent activity and cases are closed. UK Finance does not have access to individual case information and is therefore unable to make an assessment as to the accuracy of the data included and no quality assurance checks are undertaken on the data inputs. However, extensive testing, engagement with members during the development of the system, and validation with other sources of fraud data allows the conclusion that the extracted data are consistent with industry trends.
- The data presented provide a statement of the origination of fraud and scams during the stated periods, noting that the victim will not, in every case, be aware of where the initial compromise happened, and as such these figures cannot be considered definitive. Only information relating to cases that have been closed are loaded to the BPS platform, so not all incidents of scams will be included here.

10

Further Analysis of the APP Fraud Data

UK Finance collates enhanced data which provide further insight into APP scams. This data covers:

- Eight scam types: malicious payee (purchase scam, investment scam, romance scam and advance fee scam) and malicious redirection (invoice and mandate scam, CEO fraud, impersonation: police/bank staff and impersonation: other).
- Six payment types: faster payment, CHAPS, BACS (payment), BACS (standing order), intrabank ("on-us") and international.
- Four payment channels: branch, internet banking, telephone banking and mobile banking.

The data in the following sections provide a breakdown of the overall APP scam data detailed in the previous section and are not in addition to the total figures.

As with previous years our analysis includes the proportion of losses that are returned to victims across each scam type.

In October 2024 the Payment Systems Regulator (PSR) introduced new mandatory reimbursement rules and reports on the impact of its APP Scams Reimbursement Requirement every quarter. The new regulations also mean that UK Finance no longer collects or publishes data against the Contingent Reimbursement (CRM) voluntary code.

UK Finance's data covers a wider range of payments and account types than those covered by the new rules from the PSR. Some of the main differences are summarised in the table below:

UK Finance reimbursement reporting	In scope mandatory reimbursement
Payments from personal accounts and businesses of all sizes	Payments made from personal, micro-businesses and charity accounts
Payments authorised in the UK and received both in the UK and internationally	Only payments authorised in the UK and received in a UK account
Payments of any value	Payments up to a value of £85,000 and claims must be made within 13 months of the payment
Payment executed through faster payments, CHAPS, BACS and international payment schemes	Payment executed through the UK faster payment system and CHAPS* systems
	*(CHAPS rules are operated by the Bank of England)

Purchase Scam

Value = £118.1m (20%)

Cases = 175,809 (5%)

In a purchase scam, the victim pays in advance for goods or services that are never received. These scams usually involve the victim using an online platform such as an auction website or social media.

Common scams include a criminal posing as the seller of a car or a technology product, such as a phone or computer, which they advertise at a low price to attract buyers. Criminals also advertise items such as fake holiday rentals and concert tickets. While many online platforms offer secure payment options, the criminal will persuade their victim to pay via a bank transfer instead. When the victim transfers the money, the seller disappears, and no goods or services arrive.

Purchase Scam 2020-2025

Purchase Scam		2020	2021	2022	2023	2024	2025	Change
Cases	Personal	80,214	97,382	114,417	152,837	163,534	171,631	5%
	Non-Personal	4,078	2,351	2,753	3,679	3,264	4,178	28%
	Total	84,292	99,733	117,170	156,516	166,798	175,809	5%
Payments	Personal	102,325	129,442	155,451	214,690	234,956	256,388	9%
	Non-Personal	5,168	2,969	3,667	4,904	4,835	6,488	34%
	Total	107,493	132,411	159,118	219,594	239,791	262,876	10%
Value	Personal	£44.7m	£56.8m	£59.6m	£77.0m	£87.9m	£106.8m	21%
	Non-Personal	£6.5m	£7.4m	£7.4m	£8.9m	£10.7m	£11.3m	6%
	Total	£51.1m	£64.1m	£67.0m	£85.9m	£98.7m	£118.1m	20%
Returned to victim	Personal	£13.0m	£18.9m	£35.3m	£51.6m	£56.3m	£85.1m	51%
	Non-Personal	£1.6m	£2.0m	£2.8m	£4.2m	£4.5m	£6.7m	49%
	Total	£14.6m	£20.9m	£38.1m	£55.8m	£60.7m	£91.8m	51%

Key Stats/Insights

- Highest loss total ever reported.
- Highest case total ever reported.
- 71% of all APP scam cases were purchase scams in 2025.
- Lowest average case value of £671 of all eight APP scam types, however this has increased from £549 in 2023 as criminals target larger amounts of money.
- 78% of all losses related to purchase scams were returned to the victim in 2025.

Investment Scam

Value = £221.5m (40%)

Cases = 14,893 (26%)

In an investment scam, a criminal convinces their victim to move their money to a fictitious fund or to pay for a fake investment. The criminal will usually promise a high return to entice their victim into making the transfer. These scams include investment in items such as gold, property, carbon credits, cryptocurrencies, land banks and wine.

The criminals behind investment scams often use cold calling to target their victim and pressurise them to act quickly by claiming the opportunity is time limited. Adverts on social media usually offering unrealistic returns, and letters are also used heavily in investment scams.

Investment Scam 2020-2025

Investment Scam		2020	2021	2022	2023	2024	2025	Change
Cases	Personal	7,900	11,905	9,941	10,060	11,608	14,603	26%
	Non-Personal	281	169	144	166	201	290	44%
	Total	8,181	12,074	10,085	10,226	11,809	14,893	26%
Payments	Personal	19,322	35,071	30,065	32,780	40,827	55,682	36%
	Non-Personal	601	594	446	616	759	1,531	102%
	Total	19,923	35,665	30,511	33,396	41,586	57,213	38%
Value	Personal	£103.6m	£166.2m	£109.3m	£98.6m	£140.1m	£203.8m	45%
	Non-Personal	£5.8m	£5.5m	£4.8m	£9.3m	£18.0m	£17.6m	-2%
	Total	£109.4m	£171.7m	£114.1m	£107.8m	£158.1m	£221.5m	40%
Returned to victim	Personal	£39.0m	£72.7m	£56.9m	£56.3m	£69.5m	£99.3m	43%
	Non-Personal	£1.2m	£2.0m	£1.7m	£2.7m	£3.8m	£7.2m	91%
	Total	£40.2m	£74.6m	£58.6m	£59.0m	£73.3m	£106.5m	45%

Key Stats/Insights

- Highest loss total ever reported.
- Highest case total ever reported.
- 38% of all APP scam losses were investment scams in 2025.
- Investment scams are being driven by fraudulent adverts/social media posts offering significant returns on investments.
- Typically victims of investment scams take longer to identify the scam compared with other APP fraud types, and whilst we are reporting increases in the current period many of these scams are likely to have been initiated prior to this.
- 48% of all losses related to investment scams were returned to the victim in 2025.

Romance Scam

Value = £39.2m (23%)

Cases = 6,335 (22%)

In a romance scam, the victim is persuaded to make a payment to a person they have met, often online through social media or dating websites and with whom they believe they are in a relationship.

Fraudsters will use fake profiles to target their victims to start a relationship, which they will try to develop over a longer period. Once they have established their victim's trust, the criminal will then claim to be experiencing a problem, such as an issue with a visa, health issues or flight tickets and ask for money to help.

Romance Scam 2020 – 2025

Romance Scam		2020	2021	2022	2023	2024	2025	Change
Cases	Personal	2,252	3,245	3,617	4,134	5,177	6,298	22%
	Non-Personal	73	25	32	26	33	37	12%
	Total	2,325	3,270	3,649	4,160	5,210	6,335	22%
Payments	Personal	12,778	25,723	30,119	39,395	49,013	61,072	25%
	Non-Personal	407	91	101	183	263	429	63%
	Total	13,185	25,814	30,220	39,578	49,276	61,501	25%
Value	Personal	£17.3m	£30.6m	£30.9m	£36.1m	£31.0m	£38.7m	25%
	Non-Personal	£0.5m	£0.3m	£0.4m	£0.4m	£0.8m	£0.5m	-35%
	Total	£17.8m	£30.9m	£31.3m	£36.5m	£31.8m	£39.2m	23%
Returned to victim	Personal	£6.5m	£12.4m	£16.3m	£22.6m	£19.4m	£25.8m	33%
	Non-Personal	£0.1m	£0.2m	£0.2m	£0.3m	£0.4m	£0.3m	-14%
	Total	£6.6m	£12.6m	£16.4m	£22.9m	£19.8m	£26.2m	32%

Key Stats/Insights

- Highest loss total ever reported.
- Highest case total ever reported and the fifth consecutive year an increase has been reported.
- 9.7 payments on average per scam; the highest of all eight scam types, demonstrating that criminals build up trust over a period, usually targeting smaller amounts to begin with.
- 67% of all losses related to romance scams were returned to the victim in 2025.

Advance Fee Scam

Value = £58.4m (65%)

Cases = 24,080 (38%)

In an advance fee scam, a criminal convinces their victim to pay a fee which they claim will result in the release of a much larger payment or as a deposit for high-value goods and holidays. These scams include claims from the criminals that the victim has won an overseas lottery, that gold or jewellery is being held at customs or that an inheritance is due.

The fraudster tells the victims that a fee must be paid to release the funds or goods, however, when the payment is made, the promised goods or money never materialise. These scams often begin on social media or with an email, or a letter sent by the criminal to the victim.

Advance fee Scam 2020-2025

Advance Fee Scam		2020	2021	2022	2023	2024	2025	Change
Cases	Personal	13,316	19,950	26,871	23,526	17,126	23,645	38%
	Non-Personal	517	545	458	323	334	435	30%
	Total	13,833	20,495	27,329	23,849	17,460	24,080	38%
Payments	Personal	22,434	36,166	50,463	50,223	39,961	82,310	106%
	Non-Personal	798	804	768	737	793	951	20%
	Total	23,232	36,970	51,231	50,960	40,754	83,261	104%
Value	Personal	£21.2m	£30.8m	£30.7m	£29.4m	£32.4m	£56.0m	73%
	Non-Personal	£1.0m	£1.4m	£1.5m	£2.0m	£2.9m	£2.4m	-17%
	Total	£22.2m	£32.1m	£32.2m	£31.3m	£35.3m	£58.4m	65%
Returned to victim	Personal	£7.4m	£10.9m	£17.2m	£20.4m	£18.8m	£33.7m	79%
	Non-Personal	£0.3m	£0.9m	£0.6m	£0.8m	£1.5m	£1.2m	-17%
	Total	£7.7m	£11.8m	£17.8m	£21.2m	£20.3m	£34.9m	72%

Key Stats/Insights

- Highest loss total ever reported.
- Highest case total reported since 2022.
- Intelligence suggests that this is being driven by criminals that are targeting deposits for high value goods such as motor vehicles and holiday rentals which do not actually exist.
- 60% of all losses related to advance fee scams were returned to the victim in 2025.

Invoice & Mandate Scam

Value = £41.3m (-4%)

Cases = 2,305 (-2%)

In an invoice or mandate scam, the victim attempts to pay an invoice to a legitimate payee, but the criminal intervenes to convince the victim to redirect the payment to an account they control.

It includes criminals targeting consumers posing as conveyancing solicitors, builders, and other tradespeople, or targeting businesses posing as a supplier, and claiming that the bank account details have changed. This type of fraud often involves the criminal either intercepting emails or compromising an email account.

Invoice & Mandate Scam 2020-2025

Invoice & Mandate Scam		2020	2021	2022	2023	2024	2025	Change
Cases	Personal	2,903	2,555	1,871	1,485	1,054	1,088	3%
	Non-Personal	1,818	1,775	1,469	1,625	1,307	1,217	-7%
	Total	4,721	4,330	3,340	3,110	2,361	2,305	-2%
Payments	Personal	3,904	3,676	2,836	2,176	1,515	1,637	8%
	Non-Personal	2,416	2,491	2,129	2,233	1,883	2,092	11%
	Total	6,320	6,167	4,965	4,409	3,398	3,729	10%
Value	Personal	£25.1m	£19.9m	£15.0m	£15.3m	£10.7m	£13.3m	24%
	Non-Personal	£43.6m	£36.8m	£34.5m	£35.0m	£32.3m	£28.0m	-13%
	Total	£68.8m	£56.7m	£49.5m	£50.3m	£43.1m	£41.3m	-4%
Returned to victim	Personal	£14.3m	£11.8m	£12.4m	£12.4m	£8.6m	£9.4m	10%
	Non-Personal	£15.4m	£10.8m	£14.0m	£11.1m	£12.5m	£10.6m	-15%
	Total	£29.8m	£22.5m	£26.4m	£23.5m	£21.1m	£20.0m	-5%

Key Stats/Insights

- Lowest loss total ever reported.
- Lowest case total ever reported.
- 68 per cent (£28 million) of invoice and mandate scam losses occurred on a non-personal or business account. Typically, businesses make genuine higher-value payments more regularly, making it harder to spot and stop a fraudulent one.
- 48% of all losses related to invoice & mandate scams were returned to the victim in 2025.

CEO Scam

Value = £5.6m (-53%)

Cases = 197 (-29%)

CEO fraud is where the scammer manages to impersonate the CEO or other high-ranking official of the victim's organisation to convince the victim to make an urgent payment to the scammer's account.

This type of fraud mostly affects businesses. To commit the fraud, the criminal will either access the company's email system or use spoofing software to email a member of the finance team with what appears to be a genuine email from the CEO. The message commonly requests a change to payment details or for a payment to be made urgently to a new account.

CEO Scam 2020-2025

CEO Scam		2020	2021	2022	2023	2024	2025	Change
Cases	Personal	82	65	50	29	36	26	-28%
	Non-Personal	275	396	382	382	241	171	-29%
	Total	357	461	432	411	277	197	-29%
Payments	Personal	127	99	80	36	109	36	-67%
	Non-Personal	360	579	535	555	343	216	-37%
	Total	487	678	615	591	452	252	-44%
Value	Personal	£0.9m	£1.1m	£0.6m	£0.3m	£0.7m	£0.7m	-4%
	Non-Personal	£3.9m	£11.6m	£12.9m	£11.2m	£11.1m	£4.8m	-56%
	Total	£4.8m	£12.7m	£13.4m	£11.6m	£11.9m	£5.6m	-53%
Returned to victim	Personal	£0.5m	£0.7m	£0.3m	£0.1m	£0.3m	£0.0m	-83%
	Non-Personal	£1.4m	£2.1m	£3.2m	£3.0m	£2.0m	£1.1m	-47%
	Total	£1.8m	£2.8m	£3.6m	£3.1m	£2.3m	£1.1m	-51%

Key Stats/Insights

- Lowest loss total reported since 2020.
- Lowest case total ever reported.
- CEO fraud remained the least common form of APP scam in 2025, accounting for less than one per cent of total cases. A total of £5.6 million was lost, also, equivalent to less than one per cent of total APP losses.
- CEO fraud has the highest average case value of all eight scam types with an average of just over £28,000 being lost per confirmed case.
- 20% of all losses related to CEO scams were returned to the victim in 2025.

Impersonation Scam: Police or Bank Staff

Value = £55.5m (-18%)

Cases = 6,016 (-23%)

In this scam, the criminal contacts the victim purporting to be from either the police or the victim's bank and convinces the victim to make a payment to an account they control.

These scams often begin with a phone call or text message, with the fraudster claiming there has been fraud on the victim's account, and they need to transfer the money to a 'safe account' to protect their funds. However, the criminal controls the recipient account. Criminals may pose as the police and ask the individual to take part in an undercover operation to investigate 'fraudulent' activity at a branch.

To commit this fraud, the criminal will often research their victim first, including using information gathered from other scams and data breaches to make their approach sound genuine.

Impersonation Scam: Police or Bank Staff 2020-2025

Impersonation Police / Bank		2020	2021	2022	2023	2024	2025	Change
Cases	Personal	20,199	28,629	16,413	10,088	7,472	5,690	-24%
	Non-Personal	978	777	535	506	317	326	3%
	Total	21,177	29,406	16,948	10,594	7,789	6,016	-23%
Payments	Personal	37,232	60,931	47,139	29,237	20,039	18,211	-9%
	Non-Personal	3,365	1,875	1,391	1,515	792	985	24%
	Total	40,597	62,806	48,530	30,752	20,831	19,196	-8%
Value	Personal	£84.3m	£130.3m	£100.7m	£67.8m	£63.0m	£50.0m	-21%
	Non-Personal	£6.6m	£7.0m	£9.1m	£11.1m	£4.9m	£5.5m	13%
	Total	£90.9m	£137.3m	£109.8m	£78.9m	£67.9m	£55.5m	-18%
Returned to victim	Personal	£48.3m	£75.4m	£76.0m	£55.3m	£44.1m	£40.2m	-9%
	Non-Personal	£3.8m	£3.9m	£6.3m	£6.1m	£3.3m	£3.9m	21%
	Total	£52.1m	£79.3m	£82.3m	£61.4m	£47.3m	£44.1m	-7%

Key Stats/Insights

- Lowest loss total ever reported.
- Lowest case total ever reported.
- Reductions likely to be caused by extensive messaging to consumers being successful, items such as advertising campaigns (e.g. Take Five to Stop Fraud), as well as key messages and warnings during the payment journey effectively educating consumers on banks' behaviours.
- 80% of all losses related to impersonation of police or bank staff scams were returned to the victim in 2025.

Impersonation Scam: Other

Value = £36.9m (-1%)

Cases = 18,435 (-7%)

In this scam, criminals claim to represent an organisation such as a utility company, communications service provider or government department. Common scams include claims that the victim must settle a fictitious fine, pay overdue tax or return an erroneous refund. Sometimes the criminal requests remote access to the victim's computer as part of the scam, claiming that they need to help 'fix' a problem.

As with police and bank staff impersonation scams, criminals will often research their targets first, using information gathered from scams, social media, and data breaches.

Impersonation Scam: Other 2020-2025

Impersonation Other		2020	2021	2022	2023	2024	2025	Change
Cases	Personal	18,341	25,233	27,463	22,534	18,850	17,585	-7%
	Non-Personal	1,387	994	956	1,028	920	850	-8%
	Total	19,728	26,227	28,419	23,562	19,770	18,435	-7%
Payments	Personal	30,824	42,643	45,608	36,557	30,764	29,932	-3%
	Non-Personal	2,510	1,983	1,468	1,621	1,327	1,473	11%
	Total	33,334	44,626	47,076	38,178	32,091	31,405	-2%
Value	Personal	£24.0m	£34.3m	£39.6m	£37.8m	£33.1m	£31.6m	-5%
	Non-Personal	£5.4m	£7.4m	£6.5m	£5.4m	£4.2m	£5.4m	28%
	Total	£55.8m	£77.5m	£67.8m	£57.3m	£37.2m	£36.9m	-1%
Returned to victim	Personal	£24.0m	£34.3m	£39.6m	£37.8m	£24.6m	£26.2m	7%
	Non-Personal	£2.1m	£2.5m	£2.7m	£2.6m	£2.4m	£3.5m	45%
	Total	£26.1m	£36.8m	£42.3m	£40.4m	£27.0m	£29.7m	10%

Key Stats/Insights

- Lowest loss total ever reported.
- Lowest case total ever reported.
- 80% of all losses related to other impersonation scams were returned to the victim in 2025.

12

Authorised Push Payment – Payment Type

This data shows the type of payment victims used to make payments in Authorised Push Payment scams.

		2020	2021	2022	2023	2024	2025	Change
Faster Payment	Payments	236,641	335,451	364,964	409,533	414,878	486,050	17%
	Value	£349.4m	£504.5m	£421.1m	£380.2m	£384.2m	£460.9m	20%
CHAPS	Payments	501	764	550	449	316	183	-42%
	Value	£14.5m	£22.5m	£13.9m	£23.1m	£15.9m	£17.6m	11%
BACs	Payments	1,193	1,695	2,227	2,530	2,134	2,929	37%
	Value	£23.5m	£20.4m	£24.0m	£27.9m	£27.2m	£19.1m	-30%
Intra bank transfer	Payments	3,113	3,358	1,242	1,646	4,868	17,959	269%
	Value	£10.6m	£7.5m	£1.5m	£2.6m	£6.7m	£9.2m	37%
International	Payments	3,123	3,869	3,283	3,302	5,983	12,312	106%
	Value	£22.7m	£28.3m	£24.7m	£25.9m	£49.9m	£69.6m	40%
Total	Payments	244,571	345,137	372,266	417,460	428,179	519,433	21%
	Value	£420.7m	£583.2m	£485.2m	£459.7m	£484.0m	£576.4m	19%

13

Authorised Push Payment – Payment Channel

This data shows the channel through which victims made the authorised push payment.

		2020	2021	2022	2023	2024	2025	Change
Branch	Payments	8,968	8,251	8,565	8,175	6,034	5,289	-12%
	Value	£43.6m	£56.6m	£45.7m	£50.0m	£40.2m	£35.8m	-11%
Internet Banking	Payments	113,853	130,016	138,700	123,458	81,306	100,083	23%
	Value	£262.5m	£329.1m	£274.6m	£224.9m	£186.9m	£218.5m	17%
Telephone Banking	Payments	5,593	6,249	6,176	6,618	3,184	3,644	14%
	Value	£17.8m	£24.4m	£15.6m	£18.9m	£20.8m	£20.3m	-2%
Mobile Banking	Payments	116,157	200,621	218,809	279,209	337,655	410,417	22%
	Value	£96.9m	£173.2m	£149.3m	£165.9m	£236.0m	£301.8m	28%
Total	Payments	244,571	345,137	372,250	417,460	428,179	519,433	21%
	Value	£420.7m	£583.2m	£485.2m	£459.7m	£484.0m	£576.4m	19%

Our Fraud Data

UK Finance publishes both the value of fraud losses and the number of cases. The data is reported to us by our members which include financial providers, credit, debit and charge card issuers, and card payment acquirers. Each incident of fraud does not equal one person being defrauded, but instead refers to the number of cards or accounts defrauded. For example, if a fraud was carried out on two cards, but they both belonged to the same person, this would represent two instances of fraud, not one.

All fraud loss figures, unless otherwise indicated, are reported as gross. This means the figures represent the total value of fraud including any money subsequently recovered by a bank.

Some caveats are required for the tables in the document.

- Comparable authorised fraud data is not available prior to 2020.
- The sum of components may not equal the total due to rounding.
- Data series are subject to restatement, based on corrections or the receipt of additional information.

Methodology for Data Collection

All of our data is collected directly from the firms we represent. We do not make any estimations (unless indicated) and have agreed definitions / reporting templates in use to ensure consistency across firms. All data submitted must pass three clear plausibility phases (below) before publication

Validation check

Datasets containing totals, sub-totals, less-than or non-nil data field rules are automatically checked by the system, highlighting erroneous data content. Such errors result in a 'failed submission' which requires amendment.

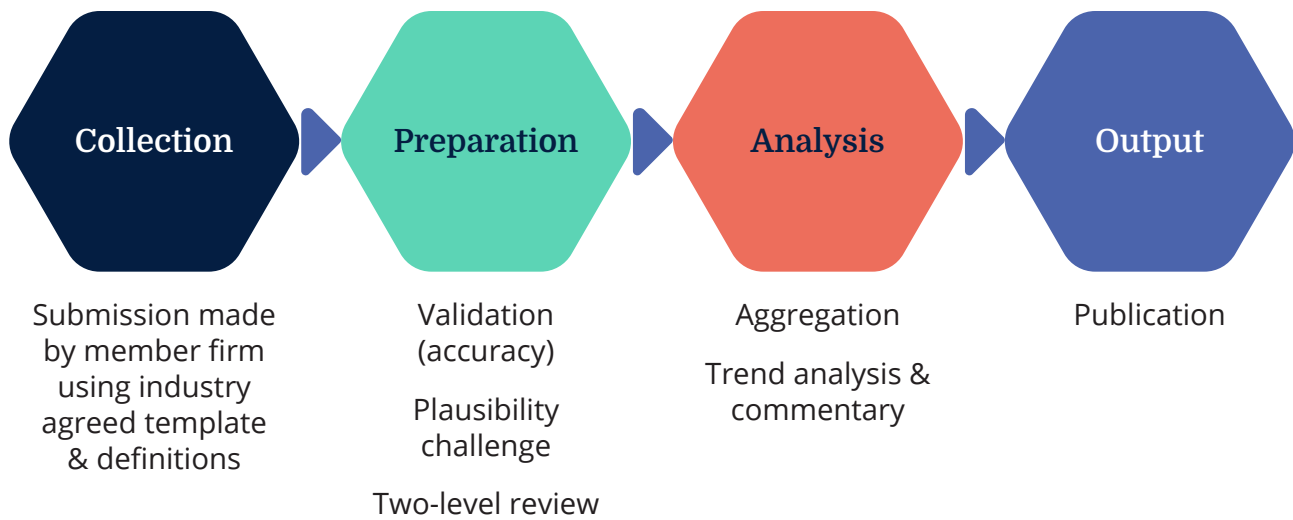
Data plausibility - inputs

Arithmetically correct data for individual members is subject to range check scrutiny against previously submitted data (automated within spreadsheets or by manual assessment) at a granular component level. Further challenge is undertaken, if possible, by (explicit or implicit) reference to alternative relevant data sources submitted by that member firm. Such subjective challenges are raised to subject matter experts and resolved with data providers

Data plausibility – outputs

For high priority, public-facing data series, data management spreadsheets incorporate visible warnings if a data observation is a series' outlier or falls outside defined tolerance intervals.

A typical process for one submission from one member would look similar to the below;



Without evidence of the above, data will not be published.

Appendix

Losses

Type	Category	Sub Category	2020	2021	2022	2023	2024	2025	Change
Unauthorised	Card	Lost & stolen	£78.9m	£77.2m	£100.2m	£104.0m	£111.7m	£109.8m	-2%
Unauthorised	Card	CNR	£4.4m	£3.9m	£4.0m	£3.0m	£3.0m	£2.8m	-4%
Unauthorised	Card	Counterfeit	£8.7m	£4.7m	£4.7m	£4.7m	£3.9m	£4.7m	21%
Unauthorised	Card	Remote purchase	£452.6m	£412.5m	£395.7m	£360.5m	£412.5m	£423.5m	3%
Unauthorised	Card	Card ID Theft	£29.7m	£26.3m	£51.7m	£79.1m	£61.5m	£54.0m	-12%
Unauthorised	Cheque	Cheque	£12.3m	£6.4m	£7.5m	£5.6m	£8.1m	£4.1m	-49%
Unauthorised	Remote Banking	Internet Banking	£159.7m	£158.3m	£114.1m	£88.7m	£77.8m	£52.6m	-32%
Unauthorised	Remote Banking	Telephone Banking	£16.1m	£15.5m	£14.7m	£17.6m	£16.7m	£7.9m	-53%
Unauthorised	Remote Banking	Mobile Banking	£21.6m	£25.8m	£34.2m	£45.5m	£49.0m	£43.9m	-10%
Authorised	Payment	Invoice & Mandate scam	£68.8m	£56.7m	£49.5m	£50.3m	£43.1m	£41.3m	-4%
Authorised	Payment	CEO scam	£4.8m	£12.7m	£13.4m	£11.6m	£11.9m	£5.6m	-53%
Authorised	Payment	Impersonation: Police/Bank	£90.9m	£137.3m	£109.8m	£78.9m	£67.9m	£55.5m	-18%
Authorised	Payment	Impersonation: Other	£55.8m	£77.5m	£67.8m	£57.3m	£37.2m	£36.9m	-1%
Authorised	Payment	Purchase scam	£51.1m	£64.1m	£67.0m	£85.9m	£98.7m	£118.1m	20%
Authorised	Payment	Investment scam	£109.4m	£171.7m	£114.1m	£107.8m	£158.1m	£221.5m	40%
Authorised	Payment	Romance scam	£17.8m	£30.9m	£31.3m	£36.5m	£31.8m	£39.2m	23%
Authorised	Payment	Advance Fee scam	£22.2m	£32.1m	£32.2m	£31.3m	£35.3m	£58.4m	65%

Cases

Type	Category	Sub Category	2020	2021	2022	2023	2024	2025	Change
Unauthorised	Card	Lost & stolen	321,994	325,501	401,340	397,549	441,582	449,189	2%
Unauthorised	Card	CNR	8,435	8,941	8,848	5,933	7,398	7,888	7%
Unauthorised	Card	Counterfeit	52,782	24,908	19,594	18,070	14,988	18,477	23%
Unauthorised	Card	Remote purchase	2,417,866	2,425,099	2,221,026	2,127,201	2,830,293	3,196,962	13%
Unauthorised	Card	Card ID Theft	34,545	38,753	82,064	142,445	115,326	103,171	-11%
Unauthorised	Cheque	Cheque	1,247	815	966	1,197	1,106	795	-28%
Unauthorised	Remote Banking	Internet Banking	55,995	72,557	32,036	13,669	9,176	9,562	4%
Unauthorised	Remote Banking	Telephone Banking	7,490	4,623	3,076	3,711	3,733	2,904	-22%
Unauthorised	Remote Banking	Mobile Banking	10,155	11,270	12,361	20,032	20,879	25,180	21%
Authorised	Payment	Invoice & Mandate scam	4,721	4,330	3,340	3,110	2,361	2,305	-2%
Authorised	Payment	CEO scam	357	461	432	411	277	197	-29%
Authorised	Payment	Impersonation: Police/Bank	21,177	29,406	16,948	10,594	7,789	6,016	-23%
Authorised	Payment	Impersonation: Other	19,728	26,227	28,419	23,562	19,770	18,435	-7%
Authorised	Payment	Purchase scam	84,292	99,733	117,170	156,516	166,798	175,809	5%
Authorised	Payment	Investment scam	8,181	12,074	10,085	10,226	11,809	14,893	26%
Authorised	Payment	Romance scam	2,325	3,270	3,649	4,160	5,210	6,335	22%
Authorised	Payment	Advance Fee scam	13,833	20,495	27,329	23,848	17,460	24,080	38%

Contributing Members

List of members who have contributed data to this publication

Allied Irish Bank

American Express

Arbuthnot Latham & Co

Bank of Ireland

Barclays Bank

C Hoare & Co

Capital One

Co-operative financial services

Coventry building society

Danske Bank

Hampden & Co

HSBC

Investec

JP Morgan Chase

Lloyds Banking Group

Marks & Spencer Money

Metro Bank

Modulr

Monzo

Nationwide Building Society

New Day

Natwest Group

Sainsburys Bank

Santander

Secure Trust Bank

HSBC Innovation Bank

Starling Bank

Barclays Tesco Bank

Triodos Bank

TSB

Vanquis

Virgin Money

Weatherbys Bank

Yorkshire Building Society

Zopa

This report is intended to provide information only and is not intended to provide financial or other advice to any person. While all reasonable efforts have been made to ensure the information contained above was correct at the time of publication, no representation or undertaking is made as to the accuracy, completeness or reliability of this report or the information or views contained in this report. None of UK Finance or its employees or agents shall have any liability to any person for decisions or actions taken based on the content of this document.

© 2026, UK Finance