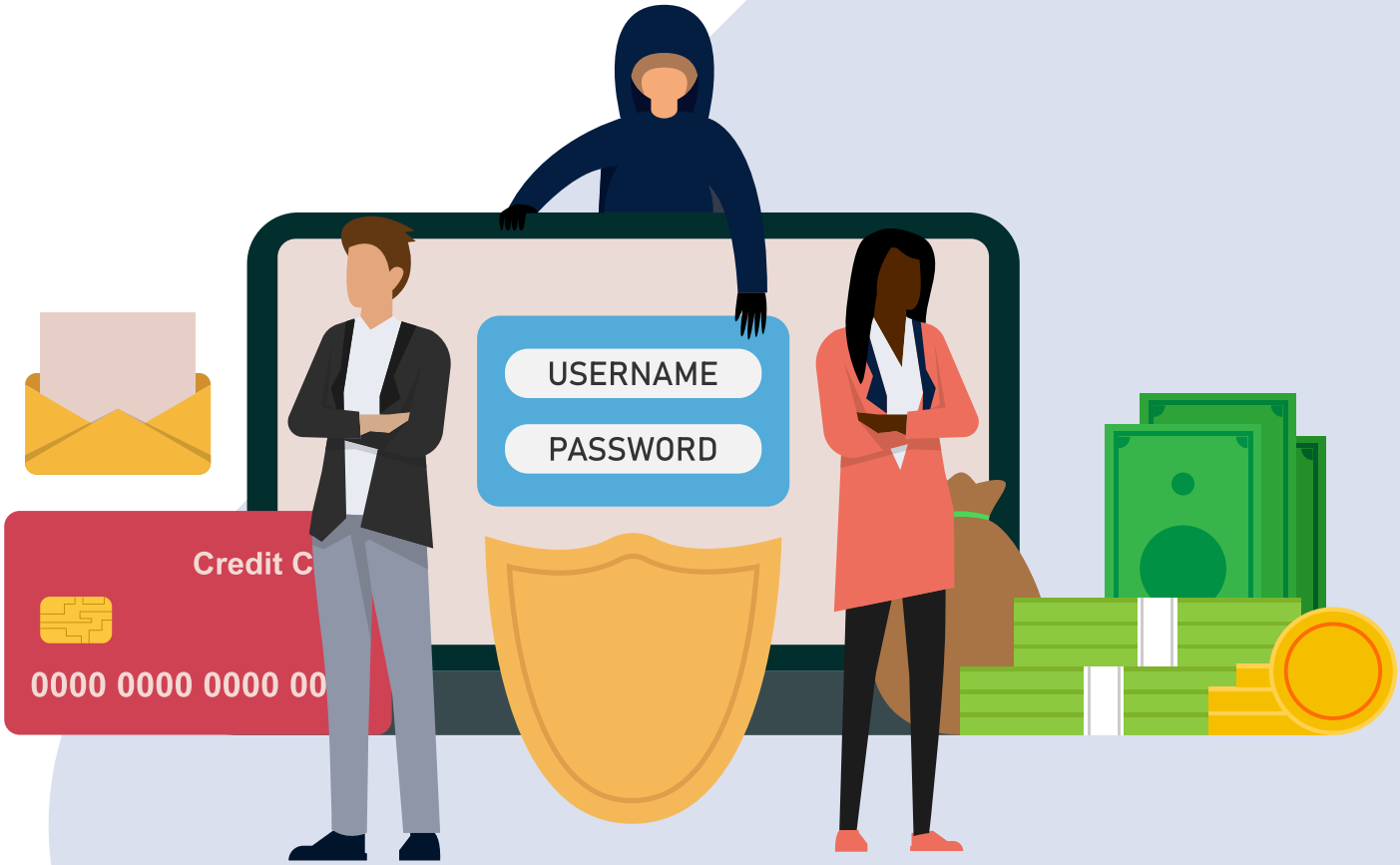
UK Finance

Annual Fraud Report 2025

In partnership with

BioCatch
Stay Safe.



Contents

UK Finance

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.

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), sanctions, anti-bribery, corruption, and cybercrime.

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 industry.

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.

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.

- Prevented values were not collected for all fraud types prior to 2015.
- 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 is not a 'victimless crime'. It causes severe harm to individuals, society, our economy, and our growth agenda. The damage caused by these crimes is greater than the financial losses, as the majority of fraud victims have their confidence ripped away and many report that their mental health has been damaged. In some tragic cases, the psychological impact of fraud can result in the loss of life through suicide. Fraud is an awful crime.

Fraud continues to be the most common crime in the UK. We have likely all suffered its consequences, either by being a victim ourselves or knowing someone who has. We all live in a society which is damaged by the organised crime groups responsible for the bulk of fraud cases, who are also involved in other types of crime which cause further individual, societal and economic harm.

The damage doesn't stop at our borders – fraud can involve appalling abuse including, as recently reported in the media, where victims are trafficked across borders and forced to work in 'scam factories', against their will and in fear of their lives.

UK Finance and our members will continue to do all that we can to protect customers and society from these terrible crimes.

Our latest figures show that Authorised Push Payment (APP) fraud, where victims are manipulated by criminals into sending them money, has fallen, both the total amount lost and the overall number of cases. We assess this was the result of a number of interventions, particularly the ongoing major investment in fraud protections by the banking and financial services industry.

Our data also shows that other types of fraud, notably remote purchase fraud, have increased. This demonstrates the longstanding principle that criminals change their tactics and, closing one vulnerability in isolation only leads them adapting and exploiting others. To fight fraud effectively, we need strong leadership and a system-wide, coordinated strategic approach.

Rather than trying to 'solve' fraud, our objective should be to protect as many people as possible by reducing and managing the evolving threat. The most effective way to achieve this is through disruption and deterrence. Gathering, developing and acting on intelligence which enables us collectively to disrupt the criminals, using a range of tactics, is the most effective way to deter these criminals from targeting the UK. Every one of us has a role to play in achieving that outcome.

The Payment Systems Regulator implemented mandatory reimbursement rules in October last year. This will increase the number of consumers being reimbursed, a positive outcome which UK Finance and our members fully support, but there is nothing to suggest it has had any impact on the perpetrators. If anything, it may have resulted in them focusing more on international payments. In addition, whilst reimbursement is a good thing for consumers, it does nothing to repair the psychological harms, nor does it protect our economy. Again, we need a system-wide, strategic approach to countering fraud, rather than tactical interventions which target individual components of the broader threat.

APP fraud involves the callous psychological exploitation of the victim, which happens online or over the telephone. This occurs long before any payment is attempted, when your bank might have the opportunity to identify it as fraud and protect you. In many respects,

our members are the last line of defence against fraud, because the online services and telecommunications sectors have opportunities to identify and disrupt these crimes long before we do.

The banking and financial services sector contributes more to the fight against fraud than any other, and if the online services and telecommunications sectors contributed to the same extent then the disruptive and deterrent impacts on criminals would be significant.

We also need the public to play their part. We all have a responsibility to keep ourselves and our families safe by protecting our personal information from criminals. We should guard our personal information as closely as we protect the keys to our homes.

The UK Finance Take Five to Stop Fraud campaign contains very helpful advice to help us all stay safe. We continue to work in close partnership with our colleagues in the Home Office on consumer education, including through their Stop! Think Fraud initiative.

The government has committed to publishing a new, expanded fraud strategy before the end of this year. We welcome this and will be calling on the government to prioritise proactive initiatives that achieve tangible outcomes. We need to bring the public and private sectors closer together and to use data and intelligence more effectively to disrupt criminals and deter them from attacking the UK.

Given many of the perpetrators are beyond the reach of our own criminal justice system, we cannot respond to fraud as we would a conventional criminal threat; the scale of this threat, and the harms it causes, means that it should be regarded as a national security issue.

Fighting fraud more effectively would have a direct positive impact on economic growth. Ensuring that the UK is a safe and attractive place to do business, and that consumers have the confidence to engage with innovative financial services products, and with the digital economy more broadly is critical. A secure financial system is inherently more investable.

Our collective priority should be preventing these crimes from happening in the first place. We need layers of defence spanning the technology, telecommunications, financial services, and public sectors.

Proactive prevention is the key to managing this national threat, because action will beat reaction 100 per cent of the time.

Ben Donaldson
Managing Director,
Economic Crime,
UK Finance

The Industry Response

The financial services industry is committed to protecting its customers from fraud, and defending the security, prosperity and reputation of the UK. The sector remains at the forefront of the fight against fraud and scams, providing deep experience, expertise and continued investment. It also works closely with other sectors, government, and law enforcement to prevent and disrupt this criminal activity and bring criminals to justice. The industry is responding to this threat through multiple activities:

Activity	Achievements
Dedicated Card and Payment Crime Unit (DCPCU) – an industry funded fully operational police unit with a national remit, formed as a collaboration between UK Finance, the City of London Police and the Metropolitan Police Service. The DCPCU has an ongoing brief to investigate, target and, where appropriate, arrest and seek successful prosecution of offenders responsible for fraud affecting the payments, banking and finance industry.	In 2024 the operational police unit saved the sector and its customers over £64.9 million, up from £33 million last year. It also disrupted 90 organised crime groups (up from 10 in 2023) and secured 75 convictions (up from 68). Case Study - Operation Henhouse: 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 OCGs who had previously been involved in serious and violent crime and have now been charged with committing fraud.
Intelligence Unit – a dedicated unit within UK Finance which shares intelligence between and across law enforcement and the banking and finance industry on emerging threats, data breaches and compromised card details.	In 2024, the Intelligence Unit disseminated 2,488,026 compromised card numbers enabling card issuers to protect their customers. The unit sent out 514 alerts to the industry and hosted 128 intelligence calls over the year. Members exchanged over 700,000 intelligence records with associated savings of £5.9m. 90% of these records were shared with Law Enforcement.
The Banking Protocol rapid response scheme – an initiative launched by UK Finance, National Trading Standards and local police forces which trains bank staff to identify the warning signs that suggest a customer may be falling victim to a scam, before alerting their local police force to intervene and investigate.	The scheme prevented £61.3million from being stolen from customers in 2024, up from £54.7million in 2023. It also resulted in 12,034 emergency calls and 136 arrests. (Case study on next page)

Activity	Achievements
	Case Study - Banking Protocol: Multiple parties were involved in the protection of a vulnerable victim in Leeds, including Leeds Anti-Social Behaviour Team, Social workers, DWP, West Yorkshire Police (WYP) safeguarding and Leeds Building Society. The incident took place in a Leeds building society branch when an elderly vulnerable male customer with learning disabilities entered and asked for a withdrawal above an agreed cap. The society colleagues were concerned that the elderly male was being financially exploited, as there were two people waiting outside the branch for him, and a change in activity was noted on the account. The branch immediately instigated banking protocol and contacted the local police. Whilst the suspects outside the branch had gone when the officers arrived, the victim advised more suspects were at his home address. WYP attended his home and officers made two arrests. It was also believed by WYP that the home address was being used for cuckooing. After collaboration with Leeds Anti-Social Behaviour Team, Social workers and DWP, the victim has now been moved to supported living accommodation and his home address has been secured by the landlord to stop further issues.
Vulnerable Victims Notification – a UK Finance/ law enforcement initiative that enables local police forces to notify financial service providers of customer vulnerabilities which may make them susceptible to fraud. Twenty-two regional police forces, fourteen banking brands and National Trading Standards have signed up to the process.	In 2024 624 notifications were received by banks from law enforcement regarding customer vulnerabilities to fraud, a 107% increase on the total number of referrals received in 2023. Six additional banks joined in 2024 taking it to 20, and currently two thirds of all police forces (30/45) are now using this process.
Best Practice Standards (BPS) System: UK Finance system recording real time information when an APP fraud occurs, including the 'enablers' of the fraud outside of the payment system. On behalf of the sector UK Finance led the industry response to the new PSR APP reimbursement rules which came into force on 7 October 2024. Through ongoing engagement and feedback, stakeholder workshops, delivery of the APP Best Practice Guide for industry, and a tactical claims management solution, it ensured that banks could process any claims from customers from day one.	There are currently 46 payment services providers participating in BPS. In 2024 160,726 cases of APP fraud were created in the system with £121.5 million returned to victims. 2024 stats provided as at 28/04/2025. There may be a minimal number of cases that are duplicated in the reporting due to them being present on different BPS workflows.

Activity	Achievements
Cross sector – collaboration with other sectors (eg telecoms, tech companies) and also working with the regulators (such as Ofcom) to drive specific data and intelligence activity to mitigate live scam attacks continues, while also ensuring effective regulation is being enacted.	**Cross sector deliverables in 2024:** • In November, the PSR announced plans to publish data on **fraud enablement**, to highlight the platforms and services that are most often exploited by fraudsters and was a welcome response to our advocacy on holding both the technology and telecoms sectors to account on fraud. • **Scams Signal** – this collaborative work with GSMA (trade association representing mobile operators) delivered the Scam Signal solution to fight fraud. The solution enables financial service providers to receive real time mobile network signals to prevent fraud/scam losses of customers who may have been targeted through social engineering calls. This has since been found to also be effective on card payments. • **Online Safety Act:** UK Finance on behalf of industry has been working closely with Ofcom to help shape the new rules on the online services measures and mandating technology solutions, a material benefit to tackling fraud in the ecosystem more effectively. • **Ofcom's Illegal Harms Statement** published in December included the DCPCU as a trusted flagger for information sharing with platforms, with Ofcom encouraging two-way data sharing.
Customer education and awareness campaigns – UK Finance delivers year-round customer education through the 'Take Five to Stop Fraud' campaign, helping people and businesses protect themselves from fraud. Education and awareness delivered to schools about money mules through the Don't be Fooled campaign.	38 major banks and building societies are currently signed up to the Take Five campaign, bringing the industry together to give people simple and consistent fraud awareness advice. In 2024 the campaign: • Ran Take Five Week when we released the ScamSceptible online tool so people can test their susceptibility to scams based on different stressors. • Hosted **Stop Inn**, physical pop-ups in London, Manchester and Glasgow, where people tested their ability to stop an action by using mind-reading technology to pour a drink. • Teamed up with Mencap to help people with learning disabilities stay safe from scams through a series of easy-read guides. • Developed resources to help raise awareness of fraud amongst people who speak English as a second language. • Launched a TikTok channel to reach new audiences. The campaign continues to deliver fraud prevention advice and education through an ongoing programme of activity. Don't Be Fooled has created primary and secondary teaching resources to educate children about the dangers and consequences of becoming a money mule. The free materials have also been specifically adapted for pupils with special educational needs and disabilities. They include classroom and assembly presentations, posters, student flyers and parent letters. The resources have been awarded the Young Enterprise Quality Mark and over 430 schools have registered to use them.

BioCatch Foreword

In these increasingly uncertain times, one thing we can all count on is the persistent nature of the fraud threat. The most recent figures from the Office of National Statistics (ONS) suggest that fraud increased by 19% last year, underlining that beyond the perspective offered by the financial services sector, the threat toward customers continues to escalate. It is incumbent on all of us to recognise that such criminality also significantly threatens the national security and prosperity of the United Kingdom.

The UK is somewhat of a bellwether for fraud, and while we can debate the causes of certain shifts, the UK Finance Annual Report highlights the industry's successes and emerging challenges.

Last year saw the introduction of mandatory reimbursement for Authorised Push Payment Fraud (APP). Aside from reducing the financial detriment suffered by consumers, the new regulation has also sought to incentivise improved detection of financial crime. APP losses fell by two per cent to just over £450 million in 2024, but case volumes also declined by 20 per cent—representing the lowest figures for cases and losses since 2021.

Notably, while APP has declined, the trend for remote purchase fraud has been reversed, likely signalling a shift in fraudsters' tactics.

With the reimbursement cost split 50/50 between the sending and receiving financial institutions, the incentive for financial institutions to identify money mules in real time has gained importance. Globally, our customers detected almost 2 million mule accounts in 2024. In many cases, that risk was identified prior to receipt of fraudulent funds.

The fight against fraud is relentless and typically asymmetrical; criminals care little for ethics, regulation, or the harm they cause. Fraud is a battle between trust and exploitation, a human challenge.

The exploitation of technology by criminals heralded an explosion in digital fraud, which now accounts for 50% of all online crime in the UK. With enforcement of the Online Safety Act still on the horizon, the role played by other sectors remains worthy of mention as it highlights that mitigating fraud risk isn't solely an issue for the financial sector.

Whilst the current threat remains severe, it would be remiss of me not to highlight forthcoming challenges, specifically the arrival of AI tools capable of autonomously planning and executing tasks. Inevitably, criminals will leverage Agentic AI, which will undoubtedly supercharge their use of existing AI tools such as large language models and generative forms of AI.

As with legitimate businesses, Agentic AI will enable criminals to scale, simplify, and cut the cost of execution. Consequently, we should anticipate that their returns will potentially increase. Identifying behavioural anomalies will be pivotal to the mitigation of this new risk.

A twelve per cent increase in fraud cases suggests that criminals have to target greater numbers of customers to achieve comparable levels of return. Whilst this likely increases their costs and consequently reduces their returns, it also has a similar impact on the sector as it strives to protect customers.

Aside from the financial impact, the 3.31 million cases recorded by UK Finance have a human cost. Many of the victims in those cases will have suffered significant

inconvenience, stress and emotional harm. We cannot measure the cost of fraud in monetary terms alone, nor should we restrict ourselves to considering the direct cost of fraud. Considering the human impact serves to underline the absolute necessity for the early detection and mitigation of financial crime.

Identifying anomalies in customer behaviour is integral to the mitigation of authorised and unauthorised fraud. Split liability also highlights the potential for closer collaboration through effective real-time data sharing. Fraud Minister Lord Hanson, in his recent keynote at the Global Anti-Scams Summit, placed emphasis on such innovation.

2024 saw the launch in Australia of the world's first inter-bank, behaviour— and device-based, fraud and scams intelligence-sharing network. We provide our customers with real-time intelligence, allowing sending institutions to review the transaction before any money leaves the sender's account.

National Australia Bank (NAB) has demonstrated the scope for behaviour to drive early interventions in payment journeys. NAB customers abandoned $48.5 million worth of payments over a two-month period following the introduction of dynamic scam warnings.

Earlier in this foreword, I observed that the fight against fraud is fundamentally asymmetrical. While this remains the case, we're proud to be part of the solution. While £1.17 billion was lost to fraudsters, a further £1.45 billion of unauthorised fraud was prevented by industry, a fifth higher than in 2023 and equivalent to 67p in every £1 attempted.

Returning to the present, despite escalating risk, it is notable that the industry's concerted efforts have successfully curtailed growth in the amount lost to criminals; regardless, they still made off with £1.17 billion.

Jonathan Frost
Director, Global Advisory,
BioCatch

01

Fraud in 2024

£1.17B

stolen through fraud in 2024, broadly unchanged from 2023

3.31M

confirmed cases, 12 per cent more than in 2023

£1.45B

of unauthorised fraud prevented by industry, up 16 per cent than in 2023 and equivalent to 67p in every £1 attempted

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	Change
Unauthorised	£783.8m	£730.4m	£726.9m	£708.7m	£722.0m	**2%**
Authorised	£420.7m	£583.2m	£485.2m	£459.7m	£450.7m	**-2%**
Total	£1204.6m	£1313.6m	£1212.1m	£1168.4m	£1172.6m	**0.4%**

Cases

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

	2020	2021	2022	2023	2024	Change
Unauthorised	2,910,509	2,912,467	2,781,311	2,734,934	3,127,951	**14%**
Authorised	154,614	195,996	207,372	232,427	185,733	**-20%**
Total	3,065,123	3,108,463	2,988,683	2,967,361	3,313,684	**12%**

*Comparable data not available for authorised fraud prior to 2020

This year's annual fraud report, which provides the most comprehensive round-up of fraud cases and losses in the UK in 2024, sees both positive and negative developments in the fight against fraud.

Overall, our latest data indicates that the total amount lost to criminals last year, across both unauthorised and authorised channels, was £1.17 billion, broadly unchanged from the total losses in 2023 and lower than losses recorded in the years 2020 to 2022. However, case numbers saw a notable twelve per cent jump last year, compared with 2023, to stand at 3.31 million (chart 1). This is the highest number of cases in our series of comparable data.

Chart 1: Total fraud cases and losses, millions

Source: UK Finance

While this points to a reduction in the average loss per case, criminals are targeting ever more victims in order to maintain flows of illicit funds with more people having to deal with the resulting stress, inconvenience and emotional harm that entails. As criminals are having to work harder to socially engineer and trick victims, as well as navigating banking and payments systems to find weaknesses, the industry was equally doing more to step up and meet that challenge.

For example, last year saw a 16 per cent increase in the amount of prevented unauthorised fraud – with increased prevention across all categories, cards, cheques, and remote banking. This figure represents fraud that was identified and stopped during the payment process and does not capture cases where effective warning messages, for example, led to a payment being abandoned earlier in the journey.

APP cases and losses down

In addition to the significant uplift in unauthorised fraud prevention, this year's data show a fall in authorised push payment (APP) fraud. This fraud type spiked during the pandemic, but the value of losses has been on a declining trend since 2021. However, even as losses were on the way down, cases continued to rise, peaking at over 230,000 in 2023.

These trends have brought about an increased focus from the banking and payments sector, and policy makers, on tackling the scourge of APP fraud and its impact on victims and society. Industry has been acting on a number of fronts, from investing in technology that can help identify and flag potentially fraudulent activity, to educating and raising awareness of risks amongst consumers, including UK Finance's Take Five campaign (see below). In addition, banking and payments firms have also sought to bring tech platforms and telecoms companies to the table, given that the vast majority of APP fraud begins outside of the industry.

From a policy perspective, a significant focus of the Payment Systems Regulator (PSR) and payment service providers has been the introduction of mandatory reimbursement of victims of APP fraud from October 7th 2024. This has required additional investment in systems to operationalise the new reimbursement rules (see Box on page 37 for further details) and further upped the ante on prevention.

In 2024, overall APP losses fell by two per cent to just over £450 million, but cases fell by a much more substantial 20 per cent – the lowest figures for both cases and losses since 2021. These declines began well in advance of implementation of the new PSR rules and can be attributed to the collective action noted above, rather than a single bullet solution, highlighting that progress requires a whole range of actions and for those to be implemented consistently right across the industry.

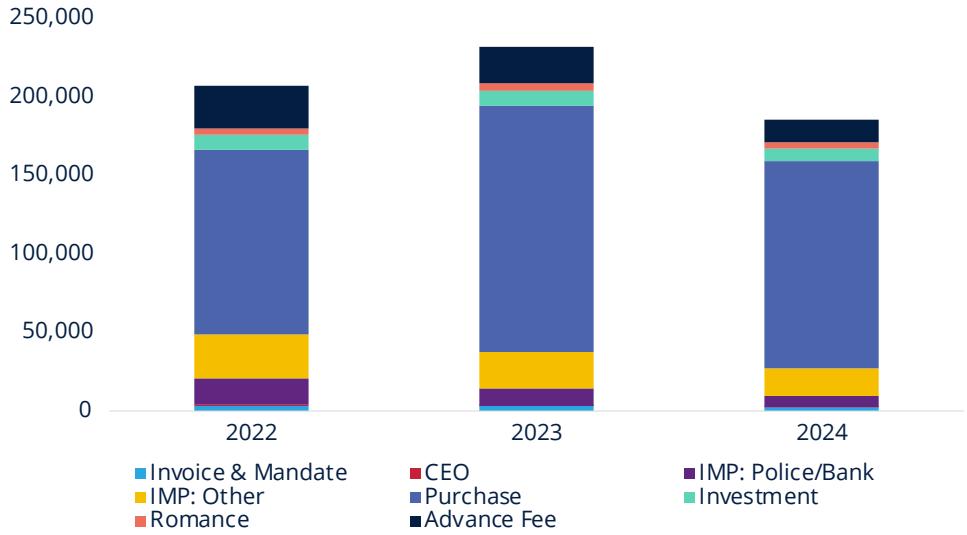
https://www.takefive-stopfraud.org.uk/

Also encouraging, as illustrated in chart 2, are the falls in APP cases across all categories and falls in losses across four of the eight categories, notably purchase and investment scams. There were increased losses in CEO fraud, which can be volatile from year to year, and a small increase in advance fee losses.

Across investment and purchase scams the fall in cases, but rise in losses, marks a change in profile of APP fraud compared with what we observed in recent years. In 2023, the story of APP fraud was one of increasing volumes of lower value, mostly purchase scam cases. For fraudsters, it was previously a numbers game, attacking a large number of victims through, for example, too good to be true purchase scams mostly originating online.

But with heightened industry attention on APP fraud, criminals have sought to extract larger sums from more 'profitable' scams. Purchase scams still account for seven in ten APP scams, despite falling 16 per cent in 2024 compared with 2023, but it has been climbing the rankings in terms of losses. A one per cent increase in losses in 2024 means purchase scams are now the second largest category by loss of all APP scam types, whereas in 2020 it was the fifth largest (out of eight). The average loss per case has risen from £606 in 2020 to £663 in 2024.

Chart 2: APP fraud by scam type, number of cases



Source: UK Finance

We see a similar trend across investment scams with cases falling by nearly a quarter in 2024 to the lowest since 2020, but a sharp 34 per cent increase in losses – the first recorded rise since 2021. Investment scams accounted for nearly a third of all APP losses last year. We noted last year that investment scams linked to cryptocurrencies have been on the rise and with increasing value and popularity, this is likely to be amongst the drivers of the loss increase in 2024.

Unlike other APP fraud categories, where we tend to see a dominant enabler of scams, victims report more varied compromise methods with around half enabled online and a quarter via telecoms channels.

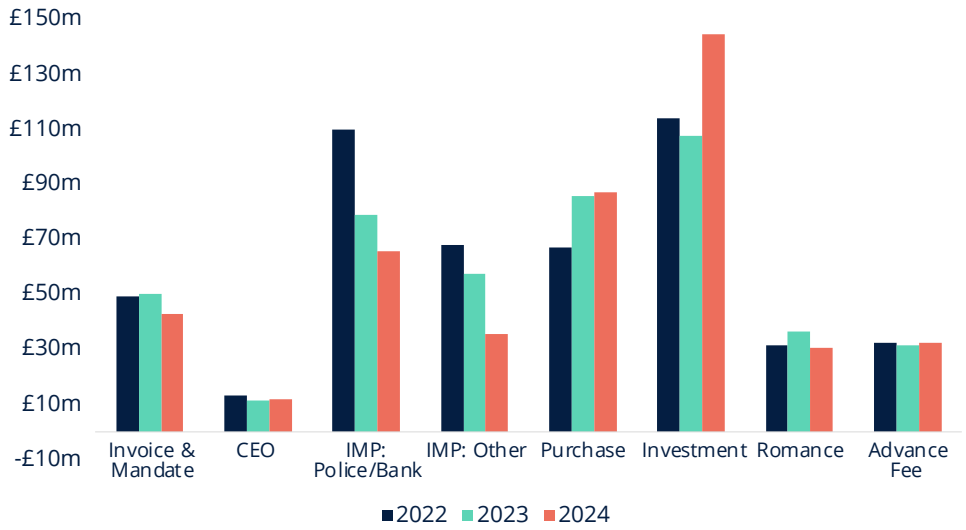
One cautionary note on investment scam cases; by nature these tend to be larger and more complex and can therefore take longer to resolve. Our data only reports closed APP cases, and as these investment scam cases are worked through, we could see an upward revision to the 2024 data in a future year as more information becomes available.

More positively, the APP categories in which we see significant downward movement in both cases and losses are romance scams, which are particularly harmful with impacts beyond the risk of financial loss, and impersonation scams.

The number of reported romance scams fell two per cent in 2024, the first fall we've seen in this series, and losses declined by a more material 17 per cent. Given that it can take some time for victims to realise they have been a targeted by fraudsters in this way, it is likely that some cases which started some years ago are still washing through our data. However, progress here is good evidence of the positive impact of education and awareness campaigns, not just by industry, but the profile of this risks of romance scams has also been regularly raised in the media.

Similarly, we also see another significant drop in impersonation fraud – both criminals impersonating police or bank staff and other forms of impersonation. Taken together both cases and losses across these categories were around a quarter lower compared with 2023. Again, we can conclude that effective warning messages, especially from banks on how they will and will not contact customers, has impacted on behaviour.

Chart 3: APP loses by scam type, £millions



Source: UK Finance

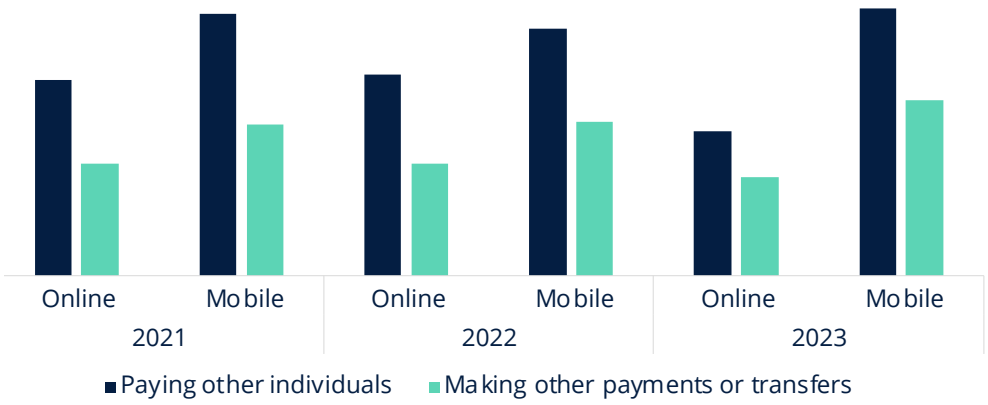
In addition to the significant progress on prevention, industry also moved at pace to implement the PSR's mandatory reimbursement rules. In preliminary reporting, the PSR found that 86 per cent of money lost to APP scams that were in scope of its rules was returned to victims between the policy becoming operational on October 7th and the end of 2024. This early trend was in line with the expectations of industry and the regulator. It is important to note that the PSR'S data is not directly comparable with UK Finance figures on APP reimbursement reported later in this report due to reporting differences and what is in scope for mandatory reimbursement.

Remote banking fraud heads lower

Turning to trends in unauthorised fraud, a further effect of the investment in fraud detection and prevention by banking and payments firms is a fall in remote banking fraud cases. This includes fraud across telephone, online, and mobile banking channels.

The use of remote banking has become business as usual for the majority of banking customers. In 2023, an estimated 87 per cent of UK adults were registered for at least one form of remote banking with mobile banking seeing the biggest rise in reported registered users in 2023. In addition, for remote banking users, mobile channels are the most common for people transferring money and making payments (chart 4).

Chart 4: Services used by remote banking users, percentage of those using each channel

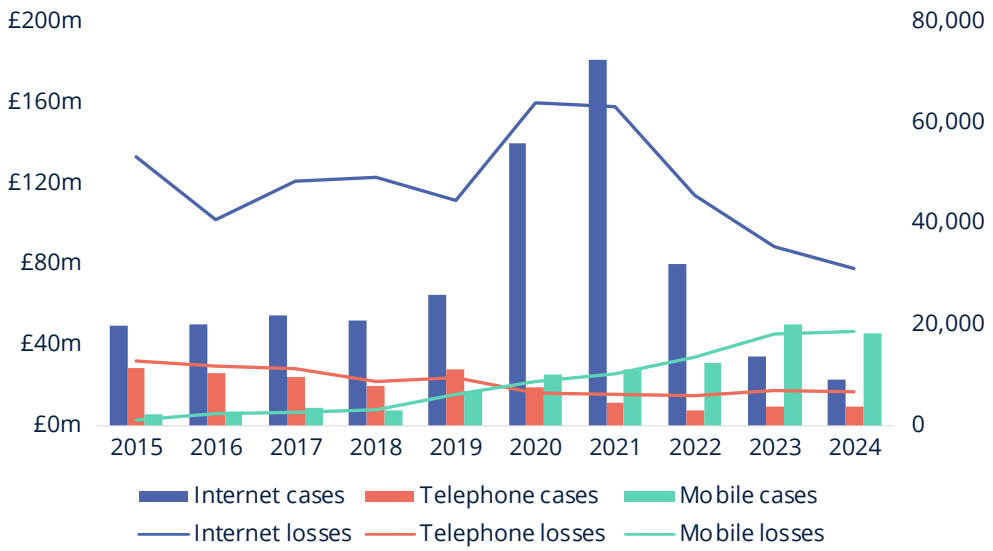


Source: UK Finance

In line with increasing adoption, we have previously seen a steady, corresponding rise in mobile banking fraud. However, the tide may have started to turn in 2024 with our data pointing to a nine per cent fall in the number of cases involving mobile banking and only a modest 3 per cent increase in losses (this compares with the 33 per cent rise seen in 2023). This fall is likely to have been driven by the same factors that have contributed to reductions in APP fraud.

The decline in mobile banking cases brings it in line with other forms of remote banking – 2024 also marked the fourth consecutive year of falls in internet banking fraud cases and losses, while fraud via telephone banking has been broadly stable over the same period (see chart 5). Overall, fraud cases and losses across all forms of remote banking declined 17 per cent and seven per cent respectively, taking both to the lowest levels reported since we began collecting this data in 2015. Additionally, nearly £250 million of losses was prevented, 14 per cent up on the previous year.

Chart 5: Remote banking cases and losses, £millions and number



Source: UK Finance

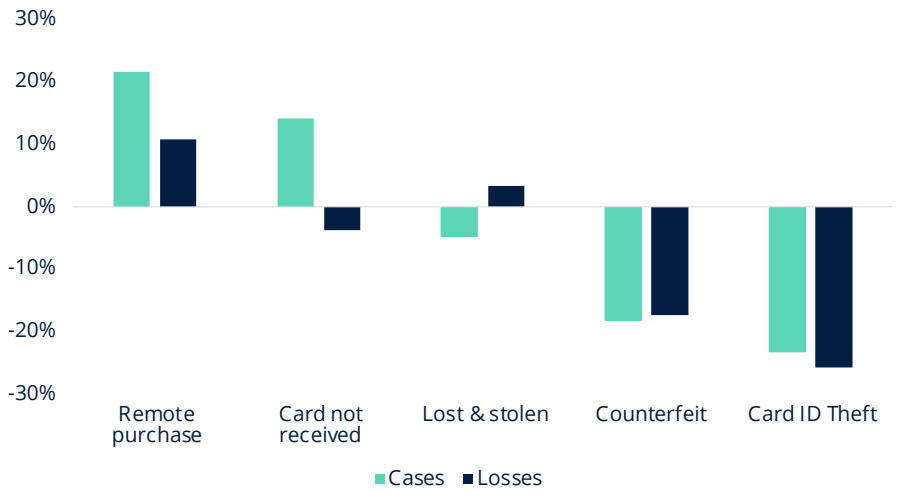
These trends should continue to give consumers confidence that firms are focused on the security of these banking channels, and that they offer a safe and convenient way to access banking and payment services.

But....remote purchase card fraud heads higher

As we have highlighted in previous reports, as fraud becomes more difficult in one avenue, as a result of improved awareness or detection, criminals' tactics will adapt, and they will use new ways to compromise individuals and exploit any system weakness.

And we see evidence of this in the rise of card fraud in 2024 – this is the flip side of the progress on APP fraud. Total unauthorised card fraud cases had been on a downward trajectory from 2020, with a number of factors from the implementation of Secure Customer Authentication to increasing the expiry dates on cards to reduce the number of cards in transit bearing down in incidences of card fraud. But in 2024 this trend reversed, and our data shows a 15 per cent increase in the number of cases and a four per cent increase in losses (chart 6).

Chart 6: Card fraud losses and cases, percentage change in 2024



Source: UK Finance

By far the largest driver of this rise was a 22 per cent increase in remote purchase fraud cases, with losses up by 11 per cent compared with 2023. With over two and a half million cases of remote purchase fraud in 2024, this is greater than incidences of card fraud across all categories prior to 2018. In contrast to the shift we saw in APP fraud towards lower volumes of higher value cases, remote purchase fraud is moving in the other direction – high volume, low value cases. The average remote purchase case value has more than halved since 2015 from around £354 to £155.

Our data indicates that around four-fifths of the cases were related to e-commerce and split roughly evenly between authenticated and non-authenticated. Our discussions with industry point to an increase in the compromise of one-time passcodes (OTPs), which are used to register digital wallets and compromise cards. This perhaps points to an over-confidence in OTPs and the protection they offer customers, which is now being exploited to a growing degree by criminals. In last year's report, we had indicated the risks around fraudsters' circumventing these protections, using sophisticated social engineering techniques to trick customers into divulging their one-time passcodes so they can authenticate fraudulent online card transactions. Developments in 2024 would suggest that this has stepped up a gear and the risk of further increases is one that industry is alive to.

Across other types of card fraud, data point to either stable or declining trends in other categories over the past year. Card ID theft cases and losses have fallen back after a spike in 2023. Also continuing to decline are instances of counterfeit fraud. Instances of lost and stolen card fraud continued to drop back in 2024, for the second year running, though there was a small increase in the level of losses. Encouragingly, and linked to trends in lost and stolen fraud, cases of fraud using contactless also fell last year, despite a four per cent increase in the number of transactions on UK-issued cards over the same period.

The rise in unauthorised card fraud, therefore, is very much down to developments in remote purchase fraud. In further evidence of the scale of escalation in attack levels on cards, the amount of card fraud prevented by industry also saw a material 12 per cent increase to over £1.45 billion, or 67p in every £1 attempted.

Fighting fraud on all fronts

This year's data offers some reassurance that concerted efforts by industry can move the needle on fraud losses – vital to stemming the flow of funds to criminals and limiting the harm to individuals. The progress made on bearing down on APP fraud is testament to that.

But it also highlights the ability of fraudsters to adapt and evolve tactics to compromise individuals by other means. This perhaps offers two lessons for policy makers and stakeholders in the fight against fraud. Firstly, we cannot assume the battle on APP fraud has been won – ongoing investment in the solutions that identify and prevent fraud will remain a priority and we need to ensure that efforts to educate consumers do not fade into the background.

Secondly, if industry's focus pivots to one particular type of activity, so will the tactics of criminals. Future strategies must, therefore, take a broad-based approach, working across the spectrum of fraud to make the UK more secure.

02

Unauthorised Fraud Summary

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

- Unauthorised fraud losses were £722 million in 2024 an increase of two per cent from 2023.
- There were 3.13 million confirmed cases of unauthorised fraud reported in 2024, a 14 per cent rise on the total reported in 2023.
- The industry prevented a further £1.45 billion of unauthorised fraud – equivalent to 67p in every £1 of attempted unauthorised fraud being stopped without a loss occurring.

Cards

Prevented: £1.15bn (12%)
Gross: £572.6m (4%)
Case: 3,095,687 (15%)

Cheques

Prevented: £53.7m (336%)
Gross: £8.1m (44%)
Case: 1,106 (-8%)

Remote Banking

Prevented: £247.6m (14%)
Gross: £141.3m (-7%)
Case: 31,158 (-17%)

03 Unauthorised Card Fraud

Debit, Credit and other payment cards

This section covers all types of unauthorised card losses. Fraud losses on UK-issued cards totalled £572.6 million in 2024, a four per cent rise from £551.3 million in 2023.

Losses

Total value of gross losses

Values	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	Change
Prevented	£843.5m	£986.0m	£984.8m	£1126.4m	£1007.5m	£983.4m	£966.6m	£974.2m	£1021.6m	£1148.3m	**12%**
Lost & stolen	£74.1m	£96.3m	£92.9m	£95.1m	£94.8m	£78.9m	£77.2m	£100.2m	£104.0m	£107.5m	**3%**
CNR	£11.7m	£12.5m	£10.2m	£6.3m	£5.2m	£4.4m	£3.9m	£4.0m	£3.0m	£2.9m	**-4%**
Counterfeit	£45.7m	£36.9m	£24.2m	£16.3m	£12.8m	£8.7m	£4.7m	£4.7m	£4.7m	£3.9m	**-17%**
Remote purchase	£398.4m	£432.3m	£408.4m	£506.4m	£470.2m	£452.6m	£412.5m	£395.7m	£360.5m	£399.6m	**11%**
Card ID Theft	£38.2m	£40.0m	£29.8m	£47.3m	£37.7m	£29.7m	£26.3m	£51.7m	£79.1m	£58.7m	**-26%**
Total	**£568.1m**	**£618.1m**	**£565.4m**	**£671.4m**	**£620.6m**	**£574.2m**	**£524.5m**	**£556.3m**	**£551.3m**	**£572.6m**	**4%**
UK fraud	£379.7m	£417.9m	£407.5m	£496.6m	£449.9m	£414.5m	£384.0m	£416.2m	£416.8m	£418.4m	**0.4%**
International fraud	£188.4m	£200.1m	£158.0m	£174.8m	£170.7m	£159.7m	£140.5m	£140.1m	£134.5m	£154.2m	**15%**

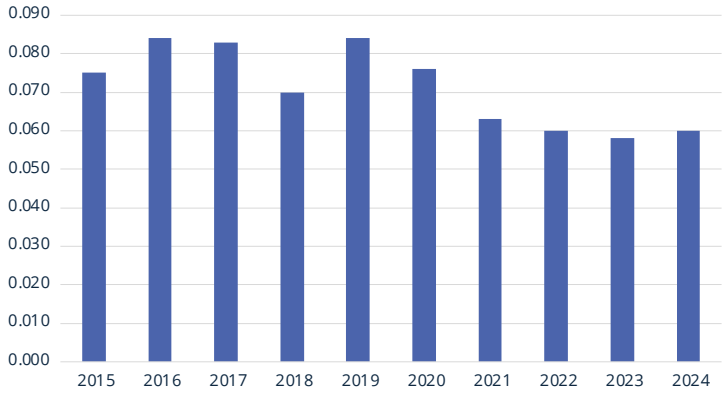
Cases

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

Cases	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	Change
Lost & stolen	143,802	231,164	350,279	434,991	460,142	321,994	325,501	401,340	397,549	378,591	**-5%**
CNR	10,719	11,377	10,903	10,046	7,907	8,435	8,941	8,848	5,933	6,772	**14%**
Counterfeit	86,021	108,597	85,025	58,636	65,907	52,782	24,908	19,594	18,070	14,763	**-18%**
Remote purchase	1,113,084	1,437,832	1,398,153	2,050,275	2,157,418	2,417,866	2,425,099	2,221,026	2,127,201	2,586,217	**22%**
Card ID Theft	33,566	31,756	29,156	63,791	54,165	34,545	38,753	82,064	142,445	109,344	**-23%**
Total	**1,387,192**	**1,820,726**	**1,873,516**	**2,617,739**	**2,745,539**	**2,835,622**	**2,823,202**	**2,732,872**	**2,691,198**	**3,095,687**	**15%**

Fraud to turnover ratio

Year	Ratio	Change
2015	0.075	**3%**
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%**



04 Analysis by Unauthorised Card Fraud Case Type

Lost and Stolen Card Fraud

Value = £107.5m (+3%) **Cases = 378,591 (-5%)**

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.

Lost and Stolen	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	Change
Value	£74.1m	£96.3m	£92.9m	£95.1m	£94.8m	£78.9m	£77.2m	£100.2m	£104.0m	£107.5m	**3%**
Cases	143,802	231,164	350,279	434,991	460,142	321,994	325,501	401,340	397,549	378,591	**-5%**

Notes:

- Loss total highest ever reported
- One third of all lost & stolen fraud spend is contactless

Card not received

Value = £2.9m (-4%) **Cases = 6,772 (+14%)**

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. This often occurs in properties with communal letterboxes, such as flats, and student halls of residence.

Card not received	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	Change
Value	£11.7m	£12.5m	£10.2m	£6.3m	£5.2m	£4.4m	£3.9m	£4.0m	£3.0m	£2.9m	**-4%**
Cases	10,719	11,377	10,903	10,046	7,907	8,435	8,941	8,848	5,933	6,772	**14%**

Notes:

- Loss total lowest ever reported
- Banks now issuing cards with five year expiry dates, resulting in fewer cards in transit and therefore reduced opportunities for them to be intercepted.

Counterfeit Card Fraud

Value = £3.9m (-17%) **Cases = 14,763 (-18%)**

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

Counterfeit Card	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	Change
Value	£45.7m	£36.9m	£24.2m	£16.3m	£12.8m	£8.7m	£4.7m	£4.7m	£4.7m	£3.9m	**-17%**
Cases	86,021	108,597	85,025	58,636	65,907	52,782	24,908	19,594	18,070	14,763	**-18%**

Notes:

- Lowest totals on record for both losses and cases volumes.
- Fraud spend restricted to those countries which do not utilise chip & PIN technology.

Remote Purchase Fraud (CNP)

Value = £399.6m (+11%) **Cases = 2,586,217 (+22%)**

This fraud occurs when a criminal use stolen card details to buy something on the internet, over the phone or through mail order.

Remote Purchase (CNP)	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	Change
Value	£398.4m	£432.3m	£408.4m	£506.4m	£470.2m	£452.6m	£412.5m	£395.7m	£360.5m	£399.6m	**11%**
Cases	1,113,084	1,437,832	1,398,153	2,050,275	2,157,418	2,417,866	2,425,099	2,221,026	2,127,201	2,586,217	**22%**

Notes:

- Loss total increased for the first time since 2018.
- 80 per cent of all CNP fraud is e-commerce, with 75 per cent of that occurring at a merchant acquired outside of the UK.
- Case total highest ever recorded, driven by the increased sophistication of social engineering techniques to acquire OTP's from victims which are then used for one off transactions or to register compromised card details for digital wallets.

Card ID Theft

Value = £58.7m (-26%) **Cases = 109,344 (-23%)**

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.

Third Party Application:

Value = £19.3m (-39%) **Cases = 24,407 (+17%)**

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.

Account Takeover:

Value = £39.4m (-17%) **Cases = 84,937 (-30%)**

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

Card ID Theft	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	Change
Value	£38.2m	£40.0m	£29.8m	£47.3m	£37.7m	£29.7m	£26.3m	£51.7m	£79.1m	£58.7m	**-26%**
Cases	33,566	31,756	29,156	63,791	54,165	34,545	38,753	82,064	142,445	109,344	**-23%**

Notes:

- Total losses and cases volumes both fall after spike seen in 2023.
- Compromise of personal data continues to drive both types of Card ID theft.

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 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 Card Fraud Losses

Value = £82.1m (-7%)

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.

UK FACE TO FACE	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	Change
Value	£53.5m	£62.8m	£61.9m	£69.8m	£64.3m	£48.9m	£48.3m	£72.0m	£88.7m	£82.1m	**-7%**

Notes:

- Contactless fraud totalled £41.1m in 2024; a decrease of one per cent on 2023; the first time a reduction has been reported for this category since 2020.
- Contactless fraud on payment cards and devices represents only seven per cent of overall card fraud losses, while 74 per cent of all card transactions were contactless last year.
- The fraud to turnover ratio for contactless fraud (1.3p) remains below that for unauthorised card fraud overall (6.0p). Contactless cards, therefore, remain a convenient and secure payment method for consumers.

UK Internet / E-Commerce Card Fraud Losses

Value = £225.0m (+11%)

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.

UK Internet/Ecommerce	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	Change
Value	N/A	N/A	N/A	£254.4m	£232.6m	£242.8m	£236.1m	£220.5m	£202.4m	£225.0m	11%

Notes:

- First increase since 2020
- 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.
- Historic data prior to 2018 is not available.

UK Cash Machine Fraud Losses

Value = £25.3m (-1%)

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.

UK Cash Machine	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	Change
Value	£32.7m	£43.1m	£37.2m	£32.6m	£30.0m	£28.1m	£24.4m	£26.1m	£25.6m	£25.3m	**-1%**

Card Fraud Abroad

Value = £154.2m (+15%)

This category covers fraud occurring in locations overseas on UK-issued cards.

Card Fraud Abroad	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	Change
Value	£188.4m	£200.1m	£158.0m	£174.8m	£170.7m	£159.7m	£140.5m	£140.1m	£134.5m	£154.2m	**15%**

06 Unauthorised Cheque Fraud

Value = £8.1m (+44%) Cases = 1,106 (-8%)

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

Counterfeit cheque fraud –

Value = £1.0m (0%) Cases = 273 (-43%)

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 = £5.7m (+83%) Cases = 582 (+13%)

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.

Forged cheque fraud –

Value = £1.5m (-3%) Cases = 251 (+25%)

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

Cheque Fraud	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	Change
Prevented	£392.8m	£196.2m	£212.3m	£218.2m	£550.8m	£238.5m	£33.1m	£19.8m	£12.3m	£53.7m	**336%**
Value	£18.9m	£13.7m	£9.8m	£20.6m	£53.6m	£12.3m	£6.4m	£7.5m	£5.6m	£8.1m	**44%**
Cases	5,746	3,388	1,745	2,020	2,852	1,247	815	966	1,197	1,106	**-8%**

Notes:

- Cheque fraud accounts for only one per cent of all unauthorised fraud
- Prevented cheque fraud totalled £53.7m in 2024, meaning 87 per cent of all attempted cheque fraud was prevented without a loss occurring.

07 Unauthorised Remote Banking Fraud

Value = £141.3m (-7%) **Cases = 31,158 (-17%)**

Remote banking fraud losses are organised into three categories: internet banking, telephone banking 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.

Remote Banking Fraud	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	Change
Prevented	£524.6m	£205.4m	£261.1m	£317.7m	£268.9m	£393.8m	£365.5m	£174.1m	£218.1m	£247.6m	**14%**
Value	£168.6m	£137.0m	£156.1m	£152.9m	£150.7m	£197.3m	£199.5m	£163.1m	£151.7m	£141.3m	**-7%**
Cases	33,306	33,392	34,746	31,797	43,920	73,640	88,450	47,473	37,412	31,158	**-17%**

Notes:

- In 2024, 88 per cent of the adult population used at least one form of remote banking
- The overall prevention rate for remote banking fraud was 64 per cent in 2024

Unauthorised Internet Banking Fraud

Value = £77.8m (-12%) **Cases = 9,176 (-33%)**

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.

Internet Banking Fraud	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	Change
Value	£133.5m	£101.8m	£121.2m	£123.0m	£111.8m	£159.7m	£158.3m	£114.1m	£88.7m	£77.8m	**-12%**
Cases	19,691	20,088	21,745	20,904	25,849	55,995	72,557	32,036	13,669	9,176	**-33%**

Notes:

- Lowest loss total reported since 2013.
- Lowest case volume total ever reported.
- Internet banking 51 per cent lower than the peak reported during Covid-19 lockdowns 2020 (£159.7m)
- £161.2m of internet banking was prevented in 2024, equivalent to £6.74 in every £10 attempted being prevented without a loss occurring.
- A further £18.1m was recovered after the incident had occurred.

Unauthorised Telephone Banking Fraud

Value = £16.7m (-5%) **Cases = 3,733 (+1%)**

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

Telephone Banking Fraud	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	Change
Value	£32.3m	£29.6m	£28.4m	£22.0m	£23.6m	£16.1m	£15.5m	£14.7m	£17.6m	£16.7m	**-5%**
Cases	11,380	10,495	9,577	7,937	11,199	7,490	4,623	3,076	3,711	3,733	**1%**

Notes:

- Social engineering remains the main driver behind this type of fraud, criminals trick customers into revealing their account security details, which are then used to impersonate the genuine account holder.
- £31.6m of telephone banking fraud was prevented in 2024, equivalent to £6.54 in every £10 of attempted fraud being stopped without a loss occurring.
- A further £1.3m was recovered after the incident had occurred.

Unauthorised Mobile Banking Fraud

Value = £46.7m (+3%) **Cases = 18,249 (-9%)**

Mobile banking fraud occurs when a criminal use 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).

Mobile Banking Fraud	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	Change
Value	£2.8m	£5.7m	£6.5m	£7.9m	£15.2m	£21.6m	£25.8m	£34.2m	£45.5m	£46.7m	**3%**
Cases	2,235	2,809	3,424	2,956	6,872	10,155	11,270	12,361	20,032	18,249	**-9%**

Notes:

- Loss total highest ever reported.
- First decrease in cases volume since 2018.
- Rises are to be expected in the mobile banking channel as the level of usage increases amongst customers. Around 60 per cent of adults living in the UK now use a mobile banking app either on their telephone or tablet, up from 33 per cent in 2015, and this is likely to continue rising as people become more familiar with and comfortable with mobile banking, and the functionality offered through mobile banking improves and payment limits increase.
- £54.8m of mobile banking fraud was prevented in 2024, equivalent to £5.39 in every £10 of attempted fraud being stopped without a loss occurring.
- A further £2.8m was recovered after the incident had occurred.

08

Overall Authorised Payment Fraud

Value = £450.7m (-2%) **Cases = 185,733 (-20%)**

Overall Authorised Payment Fraud		2020	2021	2022	2023	2024	Change
Cases	Personal	145,207	188,964	200,643	224,692	179,115	**-20%**
	Non-Personal	9,407	7,032	6,729	7,735	6,618	**-14%**
	Total	154,614	195,996	207,372	232,427	185,733	**-20%**
Payments	Personal	228,946	333,751	361,761	405,096	339,271	**-16%**
	Non-Personal	15,625	11,386	10,505	12,364	10,996	**-11%**
	Total	244,571	345,137	372,266	417,460	350,267	**-16%**
Value	Personal	£347.4m	£505.9m	£408.2m	£376.4m	£365.7m	**-3%**
	Non-Personal	£73.3m	£77.4m	£77.0m	£83.3m	£84.9m	**2%**
	Total	£420.7m	£583.2m	£485.2m	£459.7m	£450.7m	**-2%**
Returned to victim	Personal	£148.9m	£233.4m	£254.1m	£256.4m	£236.7m	**-8%**
	Non-Personal	£25.8m	£24.3m	£31.5m	£30.8m	£30.3m	**-2%**
	Total	£174.7m	£257.7m	£285.6m	£287.3m	£267.1m	**-7%**

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 bank or through recovery of funds from the beneficiary account

09

APP Voluntary Code

*The figures quoted below are included within the overall APP total in the previous section and should therefore not be treated as an addition to the overall numbers.

The authorised push payment (APP) scams voluntary code was introduced on 28 May 2019, following work between the industry, consumer groups and the regulator. It provided protections for customers of signatory payment service providers (PSPs) and delivers a significant commitment from all signatory firms to reimburse victims of authorised push payment fraud in any scenario where the customer has met the standards expected of them under the code.

Ten Payment Service Providers (PSPs), representing 19 consumer brands and over 90 per cent of authorised push payments, have signed up to the code so far. A list of signatories can be found on the Lending Standards Board website.

As of October 2024, voluntary code commitments have been superseded by mandatory reimbursement regulations. This will, therefore, be the last year in which we publish separate voluntary code data on cases, losses and repayments.

In 2024, 185,733 cases were assessed and closed with a total value of £450.7 million. Our latest figures show that £267.1 million of losses were returned to victims under the APP voluntary code, accounting for 59 per cent of losses in these cases.

Voluntary Code Data	<£1k	>£1k <£10k	>£10k	Total
Cases	121,922	24,188	4,948	151,058
Payments	169,531	72,849	45,688	288,068
Value	£29.7m	£73.1m	£190.2m	£293.0m
Returned to victim	£23.6m	£49.6m	£115.6m	£201.2m*

* This includes £12.4m of reimbursement for cases where a repatriation of funds has occurred from the beneficiary account after the case has been reported and the funds are subsequently returned to the victim. It is not possible to attribute the totals to specific scam types. However, they are included to reflect the true value reimbursed to victims for those cases which have been assessed using the code

10 Fraud Enabler Data

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 the vast majority of 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:

- 70 per cent of fraud cases are enabled by online sources. These cases tend to include lower-value scams such as purchase fraud and therefore account for 29 per cent of total losses.
- 16 per cent of fraud cases are enabled by telecommunications, these are usually higher value cases such as impersonation scams and so account for 36 per cent of losses.

The analysis is based on information provided by victims of fraud and then reported by UK Finance members. A further explanation of how the data is gathered and the methodology is included below.

Fraud Enabler Data	2022		2023		2024	
	Volume	Value	Volume	Value	Volume	Value
Online	78%	36%	76%	30%	70%	29%
Telecommunications	18%	45%	16%	43%	16%	36%
Email	2%	12%	1%	11%	1%	10%
Other	1%	3%	2%	5%	3%	7%
Unable to ascertain	1%	4%	5%	11%	10%	18%

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. For more detail on these please refer to the UK Finance Annual Fraud Report.

11 Further Analysis of the APP Scam 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.

Included within each scam type is the data relating to the cases which have been assessed using the APP voluntary code.

As with previous years our analysis includes the proportion of losses that are returned to victims across each scam type, both in aggregate and by voluntary code participants.

In October 2024 the Payment Systems Regulator (PSR) introduced new mandatory reimbursement rules.

This means there were different reimbursement regimes in place throughout 2024.

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 made from personal, micro-businesses and charity accounts
Payments from personal accounts and businesses of all sizes	
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 = £87.1m (+1%) **Cases = 131,447 (-16%)**

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 2020-2024

Purchase Scam		2020	2021	2022	2023	2024	Change
Cases	Personal	80,214	97,382	114,417	152,837	128,183	**-16%**
	Non-Personal	4,078	2,351	2,753	3,679	3,264	**-11%**
	Total	84,292	99,733	117,170	156,516	131,447	**-16%**
Payments	Personal	102,325	129,442	155,451	214,690	184,598	**-14%**
	Non-Personal	5,168	2,969	3,667	4,904	4,835	**-1%**
	Total	107,493	132,411	159,118	219,594	189,433	**-14%**
Value	Personal	£44.7m	£56.8m	£59.6m	£77.0m	£76.4m	**-1%**
	Non-Personal	£6.5m	£7.4m	£7.4m	£8.9m	£10.7m	**20%**
	Total	£51.1m	£64.1m	£67.0m	£85.9m	£87.1m	**1%**
Returned to victim	Personal	£13.0m	£18.9m	£35.3m	£51.6m	£54.5m	**6%**
	Non-Personal	£1.6m	£2.0m	£2.8m	£4.2m	£4.5m	**7%**
	Total	£14.6m	£20.9m	£38.1m	£55.8m	£59.0m	**6%**

Notes:

- Loss total highest ever recorded (£87.1m)
- 71 per cent of all APP scams reported in 2024 were purchase scams accounting for 19 per cent of the value
- Reimbursement rate in 2024 was 68 per cent, up from 29 per cent in 2020.
- 85 per cent of purchase scams originated online

Purchase Scam – Voluntary code only

Only those cases assessed using the voluntary code by signatory PSPs All cases reported below are also included in previous figures relating to all purchase scam cases reported and should not be treated as an addition.

Purchase Scam VC Data	<£1k	>£1k <£10k	>£10k	Total
Cases	97,557	10,911	746	109,214
Payments	129,172	24,749	4,440	158,361
Value	£20.3m	£30.7m	£16.2m	£67.3m
Returned to victim	£16.2m	£20.0m	£9.9m	£46.2m

Notes:

- 69 per cent of all losses were returned to the victim in 2024 compared with 34 per cent in 2021
- 89 per cent of all cases assessed involved case values of less than £1,000

Investment Scam

Value = £144.4m (+34%) **Cases = 7,767 (-24%)**

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 2020-2024

Investment Scam		2020	2021	2022	2023	2024	Change
Cases	Personal	7,900	11,905	9,941	10,060	7,566	**-25%**
	Non-Personal	281	169	144	166	201	**21%**
	Total	8,181	12,074	10,085	10,226	7,767	**-24%**
Payments	Personal	19,322	35,071	30,065	32,780	28,619	**-13%**
	Non-Personal	601	594	446	616	759	**23%**
	Total	19,923	35,665	30,511	33,396	29,378	**-12%**
Value	Personal	£103.6m	£166.2m	£109.3m	£98.6m	£126.4m	**28%**
	Non-Personal	£5.8m	£5.5m	£4.8m	£9.3m	£18.0m	**95%**
	Total	£109.4m	£171.7m	£114.1m	£107.8m	£144.4m	**34%**
Returned to victim	Personal	£39.0m	£72.7m	£56.9m	£56.3m	£68.3m	**21%**
	Non-Personal	£1.2m	£2.0m	£1.7m	£2.7m	£3.8m	**40%**
	Total	£40.2m	£74.6m	£58.6m	£59.0m	£72.1m	**22%**

Notes:

- Investment scam losses increase for first time since 2021
- Reimbursement rate in 2024 was 50 per cent, up from 34 per cent in 2020
- 53 per cent of investment scams originated online in 2023, 23 per cent via a telecommunications service or platform

Investment Scam – Voluntary code only

Only those cases assessed using the voluntary code by signatory PSPs All cases reported below are also included in previous figures relating to all purchase scam cases reported and should not be treated as an addition.

Investment Scam VC Data	<£1k	>£1k <£10k	>£10k	Total
Cases	2,196	1,899	1,567	5,662
Payments	3,795	6,747	10,868	21,410
Value	£0.8m	£7.9m	£81.1m	£89.8m
Returned to victim	£0.6m	£4.9m	£44.0m	£49.4m

Notes:

- 55 per cent of all losses were returned to the victim in 2024 compared with 45 per cent in 2021

Romance Scam

Value = £30.5m (-17%) **Cases = 4,087 (-2%)**

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 – 2024

Romance Scam		2020	2021	2022	2023	2024	Change
Cases	Personal	2,252	3,245	3,617	4,134	4,054	**-2%**
	Non-Personal	73	25	32	26	33	**27%**
	Total	2,325	3,270	3,649	4,160	4,087	**-2%**
Payments	Personal	12,778	25,723	30,119	39,395	44,467	**13%**
	Non-Personal	407	91	101	183	263	**44%**
	Total	13,185	25,814	30,220	39,578	44,730	**13%**
Value	Personal	£17.3m	£30.6m	£30.9m	£36.1m	£29.7m	**-18%**
	Non-Personal	£0.5m	£0.3m	£0.4m	£0.4m	£0.8m	**93%**
	Total	£17.8m	£30.9m	£31.3m	£36.5m	£30.5m	**-17%**
Returned to victim	Personal	£6.5m	£12.4m	£16.3m	£22.6m	£19.1m	**-15%**
	Non-Personal	£0.1m	£0.2m	£0.2m	£0.3m	£0.4m	**46%**
	Total	£6.6m	£12.6m	£16.4m	£22.9m	£19.5m	**-15%**

Notes:

- Romance scams have an average of nearly 11 scam payments per case; the highest of the eight scam types, highlighting evidence that the individual is often convinced to make multiple, generally smaller, payments to the criminal over a longer period
- Reimbursement rate in 2024 was 64 per cent, up from 37 per cent in 2020
- 75 per cent of all romance scams originated online in 2024

Romance Scam – Voluntary code only

Only those cases assessed using the voluntary code by signatory PSPs. All cases reported below are also included in previous figures relating to all romance scam cases reported and should not be treated as an addition.

Romance Scam VC Data	<£1k	>£1k <£10k	>£10k	Total
Cases	1,755	1,138	462	3,355
Payments	6,286	16,306	17,230	39,822
Value	£0.6m	£4.0m	£18.4m	£22.9m
Returned to victim	£0.5m	£2.8m	£11.5m	£14.8m

Notes:

- 64 per cent of all losses were returned to the victim in 2024 compared with 44 per cent in 2021

Advance Fee Scam

Value = £32.4m (+4%) **Cases = 14,749 (-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 2020-2024

Advance Fee Scam		2020	2021	2022	2023	2024	Change
Cases	Personal	13,316	19,950	26,871	23,526	14,415	**-39%**
	Non-Personal	517	545	458	323	334	**3%**
	Total	13,833	20,495	27,329	23,849	14,749	**-38%**
Payments	Personal	22,434	36,166	50,463	50,223	34,205	**-32%**
	Non-Personal	798	804	768	737	793	**8%**
	Total	23,232	36,970	51,231	50,960	34,998	**-31%**
Value	Personal	£21.2m	£30.8m	£30.7m	£29.4m	£29.5m	**1%**
	Non-Personal	£1.0m	£1.4m	£1.5m	£2.0m	£2.9m	**49%**
	Total	£22.2m	£32.1m	£32.2m	£31.3m	£32.4m	**4%**
Returned to victim	Personal	£7.4m	£10.9m	£17.2m	£20.4m	£18.5m	**-10%**
	Non-Personal	£0.3m	£0.9m	£0.6m	£0.8m	£1.5m	**87%**
	Total	£7.7m	£11.8m	£17.8m	£21.2m	£20.0m	**-6%**

Notes:

- Reimbursement rate in 2024 was 62 per cent, up from 34 per cent in 2020
- Deposits for high value goods remain a key driver behind this scam type
- 58 per cent of advance fee scams originated online in 2024

Advance fee Scam – Voluntary code only

Only those cases assessed using the voluntary code by signatory PSPs All cases reported below are also included in previous figures relating to all advance fee scam cases reported and should not be treated as an addition.

Advance Fee VC Data	<£1k	>£1k <£10k	>£10k	Total
Cases	9,356	2,077	452	11,885
Payments	15,440	7,265	5,725	28,430
Value	£2.4m	£6.3m	£15.3m	£24.1m
Returned to victim	£1.9m	£3.8m	£8.5m	£14.3m

Notes:

- 59 per cent of all losses were returned to the victim in 2024 compared with 34 per cent in 2021

Invoice & Mandate Scam

Value = £42.7m (-15%) **Cases = 2,301 (-26%)**

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 2020-2024

Invoice & Mandate Scam		2020	2021	2022	2023	2024	Change
Cases	Personal	2,903	2,555	1,871	1,485	994	**-33%**
	Non-Personal	1,818	1,775	1,469	1,625	1,307	**-20%**
	Total	4,721	4,330	3,340	3,110	2,301	**-26%**
Payments	Personal	3,904	3,676	2,836	2,176	1,427	**-35%**
	Non-Personal	2,416	2,491	2,129	2,233	1,883	**-16%**
	Total	6,320	6,167	4,965	4,409	3,310	**-25%**
Value	Personal	£25.1m	£19.9m	£15.0m	£15.3m	£10.4m	**-32%**
	Non-Personal	£43.6m	£36.8m	£34.5m	£35.0m	£32.3m	**-8%**
	Total	£68.8m	£56.7m	£49.5m	£50.3m	£42.7m	**-15%**
Returned to victim	Personal	£14.3m	£11.8m	£12.4m	£12.4m	£8.4m	**-32%**
	Non-Personal	£15.4m	£10.8m	£14.0m	£11.1m	£12.5m	**12%**
	Total	£29.8m	£22.5m	£26.4m	£23.5m	£20.9m	**-11%**

Notes:

- 76 per cent (£32.3m) of invoice & mandate scam losses occurred on a non-personal account
- This type of fraud often involves the criminal either intercepting emails or compromising an email account, 81 per cent of all invoice & mandate scam cases reported in 2024 originated via an email
- Reimbursement rate in 2023 was 49 per cent, up from 43 per cent in 2020

Invoice & mandate Scam – Voluntary code only

Only those cases assessed using the voluntary code by signatory PSPs All cases reported below are also included in previous figures relating to all invoice & mandate scam cases reported and should not be treated as an addition.

Invoice & Mandate VC Data	<£1k	>£1k <£10k	>£10k	Total
Cases	388	549	239	1,176
Payments	447	767	504	1,718
Value	£0.2m	£1.9m	£9.7m	£11.8m
Returned to victim	£0.1m	£1.4m	£7.0m	£8.6m

Notes:

- 72 per cent of all losses were returned to the victim in 2024 compared with 61 per cent in 2021

CEO Scam

Value = £11.8m (+2%) **Cases = 270 (-34%)**

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 2020-2024

CEO Scam		2020	2021	2022	2023	2024	Change
Cases	Personal	82	65	50	29	29	**0%**
	Non-Personal	275	396	382	382	241	**-37%**
	Total	357	461	432	411	270	**-34%**
Payments	Personal	127	99	80	36	98	**172%**
	Non-Personal	360	579	535	555	343	**-38%**
	Total	487	678	615	591	441	**-25%**
Value	Personal	£0.9m	£1.1m	£0.6m	£0.3m	£0.7m	**113%**
	Non-Personal	£3.9m	£11.6m	£12.9m	£11.2m	£11.1m	**-1%**
	Total	£4.8m	£12.7m	£13.4m	£11.6m	£11.8m	**2%**
Returned to victim	Personal	£0.5m	£0.7m	£0.3m	£0.1m	£0.3m	**414%**
	Non-Personal	£1.4m	£2.1m	£3.2m	£3.0m	£2.0m	**-34%**
	Total	£1.8m	£2.8m	£3.6m	£3.1m	£2.3m	**-26%**

Notes:

- CEO scam is the smallest of all eight scam types in both loss and case volumes; accounting for only 2.6 per cent of the total loss and less than 0.2 per cent of overall case volumes
- 94 per cent of all CEO scam losses occurred on a non-personal account
- Average case value of £40,000+, the highest of all eight scam types
- Reimbursement rate in 2023 was 19 per cent, down from 38 per cent in 2020. CEO scam is the only scam type to show a reduction in the reimbursement rate when compared with previous years, given the low volumes and high values associated with this category, one large case can have a significant impact on percentage changes and this is likely to be the case here

CEO Scam – Voluntary code only

Only those cases assessed using the voluntary code by signatory PSPs All cases reported below are also included in previous figures relating to all CEO scam cases reported and should not be treated as an addition.

CEO Scam VC Data	<£1k	>£1k <£10k	>£10k	Total
Cases	19	60	23	102
Payments	20	127	47	194
Value	£0.01m	£0.3m	£0.9m	£1.3m
Returned to victim	£0.01m	£0.2m	£0.4m	£0.6m

Notes:

- 49 per cent of all losses were returned to the victim in 2024 compared with 61 per cent in 2021

Impersonation: Police / Bank Staff

Value = £65.9m (-16%) **Cases = 7,202 (-32%)**

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: Police / Bank Staff 2020-2024

Impersonation Police / Bank		2020	2021	2022	2023	2024	Change
Cases	Personal	20,199	28,629	16,413	10,088	6,885	**-32%**
	Non-Personal	978	777	535	506	317	**-37%**
	Total	21,177	29,406	16,948	10,594	7,202	**-32%**
Payments	Personal	37,232	60,931	47,139	29,237	18,403	**-37%**
	Non-Personal	3,365	1,875	1,391	1,515	792	**-48%**
	Total	40,597	62,806	48,530	30,752	19,195	**-38%**
Value	Personal	£84.3m	£130.3m	£100.7m	£67.8m	£61.0m	**-10%**
	Non-Personal	£6.6m	£7.0m	£9.1m	£11.1m	£4.9m	**-56%**
	Total	£90.9m	£137.3m	£109.8m	£78.9m	£65.9m	**-16%**
Returned to victim	Personal	£48.3m	£75.4m	£76.0m	£55.3m	£43.5m	**-21%**
	Non-Personal	£3.8m	£3.9m	£6.3m	£6.1m	£3.3m	**-47%**
	Total	£52.1m	£79.3m	£82.3m	£61.4m	£46.8m	**-24%**

Notes:

- Lowest loss total ever reported
- Lowest case volume total ever reported
- Reduction likely to be caused by extensive messaging to consumers being successful, items such as advertising campaigns (e.g. TakeFive), as well as key messages and warning messages during the payment journey effectively educating consumers on banks behaviours.
- Reimbursement rate in 2024 was 71 per cent, up from 57 per cent in 2020

Impersonation: Police / Bank – Voluntary code only

Only those cases assessed using the voluntary code by signatory PSPs All cases reported below are also included in previous figures relating to all impersonation police/bank scam cases reported and should not be treated as an addition.

Impersonation Police / Bank VC Data	<£1k	>£1k <£10k	>£10k	Total
Cases	2,037	2,541	1,165	5,743
Payments	3,558	7,543	4,823	15,924
Value	£0.95m	£9.6m	£38.3m	£48.9m
Returned to victim	£0.81m	£7.7m	£28.0m	£36.5m

Notes:

- 75 per cent of all losses were returned to the victim in 2024 compared with 60 per cent in 2020

Impersonation: Other

Value = £35.8m (-38%) **Cases = 17,910 (-24%)**

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: Other 2020-2024

Impersonation Other		2020	2021	2022	2023	2024	Change
Cases	Personal	18,341	25,233	27,463	22,534	16,989	**-25%**
	Non-Personal	1,387	994	956	1,028	921	**-10%**
	Total	19,728	26,227	28,419	23,562	17,910	**-24%**
Payments	Personal	30,824	42,643	45,608	36,557	27,454	**-25%**
	Non-Personal	2,510	1,983	1,468	1,621	1,328	**-18%**
	Total	33,334	44,626	47,076	38,178	28,782	**-25%**
Value	Personal	£24.0m	£34.3m	£39.6m	£37.8m	£24.1m	**-36%**
	Non-Personal	£5.4m	£7.4m	£6.5m	£5.4m	£4.2m	**-22%**
	Total	£55.8m	£77.5m	£67.8m	£57.3m	£35.8m	**-38%**
Returned to victim	Personal	£24.0m	£34.3m	£39.6m	£37.8m	£24.1m	**-36%**
	Non-Personal	£2.1m	£2.5m	£2.7m	£2.6m	£2.4m	**-6%**
	Total	£26.1m	£36.8m	£42.3m	£40.4m	£26.6m	**-34%**

Notes:

- Reimbursement rate in 2024 was 74 per cent; the highest of all eight scam types

Impersonation: Other – Voluntary code only

Only those cases assessed using the voluntary code by signatory PSPs All cases reported below are also included in previous figures relating to all impersonation: other scam cases reported and should not be treated as an addition.

Impersonation Other VC Data	<£1k	>£1k <£10k	>£10k	Total
Cases	8,613	5,013	294	13,920
Payments	10,812	9,345	2,051	22,208
Value	£4.48m	£12.2m	£10.1m	£26.8m
Returned to victim	£3.53m	£8.8m	£6.1m	£18.5m

Notes:

- 69 per cent of all losses were returned to the victim when assessed using the voluntary code in 2024 compared with 45 per cent in 2021

12 Payment Type

This data shows the type of payment method the victim used to make the payment in the authorised push payment scam.

		2020	2021	2022	2023	2024	Change
Faster Payment	Payments	236,641	335,451	364,964	409,533	337,371	**-18%**
	Value	£349.4m	£504.5m	£421.1m	£380.2m	£351.3m	**-8%**
CHAPS	Payments	501	764	550	449	316	**-30%**
	Value	£14.5m	£22.5m	£13.9m	£23.1m	£15.9m	**-31%**
BACs	Payments	1,193	1,695	2,227	2,530	2,126	**-16%**
	Value	£23.5m	£20.4m	£24.0m	£27.9m	£27.2m	**-2%**
Intra bank transfer	Payments	3,113	3,358	1,242	1,645	4,471	**172%**
	Value	£10.6m	£7.5m	£1.5m	£2.6m	£6.4m	**148%**
International	Payments	3,123	3,869	3,283	3,302	5,983	**81%**
	Value	£22.7m	£28.3m	£24.7m	£25.9m	£49.9m	**93%**
Total	Payments	244,571	345,137	372,266	417,459	350,267	**-16%**
	Value	£420.7m	£583.2m	£485.2m	£459.7m	£450.7m	**-2%**

Notes:

- Faster Payments was used for 96 per cent of fraudulent APP scam payments
- CHAPS was the least common payment method, representing less than one per cent of cases, the high-value nature of transactions using this payment type meant that it accounted for 3.5 per cent of the total value

13 Payment Channel

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

		2020	2021	2022	2023	2024	Change
Branch	Payments	8,968	8,251	8,565	8,175	6,034	**-26%**
	Value	£43.6m	£56.6m	£45.7m	£50.0m	£40.2m	**-20%**
Internet Banking	Payments	113,853	130,016	138,700	123,457	81,306	**-34%**
	Value	£262.5m	£329.1m	£274.6m	£224.9m	£186.9m	**-17%**
Telephone Banking	Payments	5,593	6,249	6,176	6,618	3,184	**-52%**
	Value	£17.8m	£24.4m	£15.6m	£18.9m	£20.8m	**10%**
Mobile Banking	Payments	116,157	200,621	218,809	279,209	259,743	**-7%**
	Value	£96.9m	£173.2m	£149.3m	£165.9m	£202.7m	**22%**
Total	Payments	244,571	345,137	372,250	417,459	350,267	**-16%**
	Value	£420.7m	£583.2m	£485.2m	£459.7m	£450.7m	**-2%**

Notes:

- The most common payment channel was mobile banking which accounted for 74 per cent of the payment volumes and 45 per cent of the loss, indicating the typically lower payment limits available to customers within the mobile banking channel

Contributing Members

List of members who have contributed data to this publication

- Allied Irish Bank
- American Express
- Arbuthnot
- Bank of Ireland
- Barclays Bank
- C Hoare & Co
- Capital One
- Citibank
- Co-Operative Financial Services
- Coventry Building Society
- Danske Bank
- Hampden & Co
- HSBC
- Investec
- Lloyds Banking Group
- Marks & Spencer
- Metro Bank
- Modulr
- Nationwide
- New Day
- Royal Bank of Scotland Group
- Sainsburys Bank
- Santander
- Silicon Valley Bank
- Starling Bank
- Tesco Bank
- Triodos Bank
- TSB
- Vanquis
- Virgin Money
- Weatherbys Bank
- Yorkshire Bank
- Zopa Bank

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.

- Prevented values were not collected for all fraud types prior to 2015.
- 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.

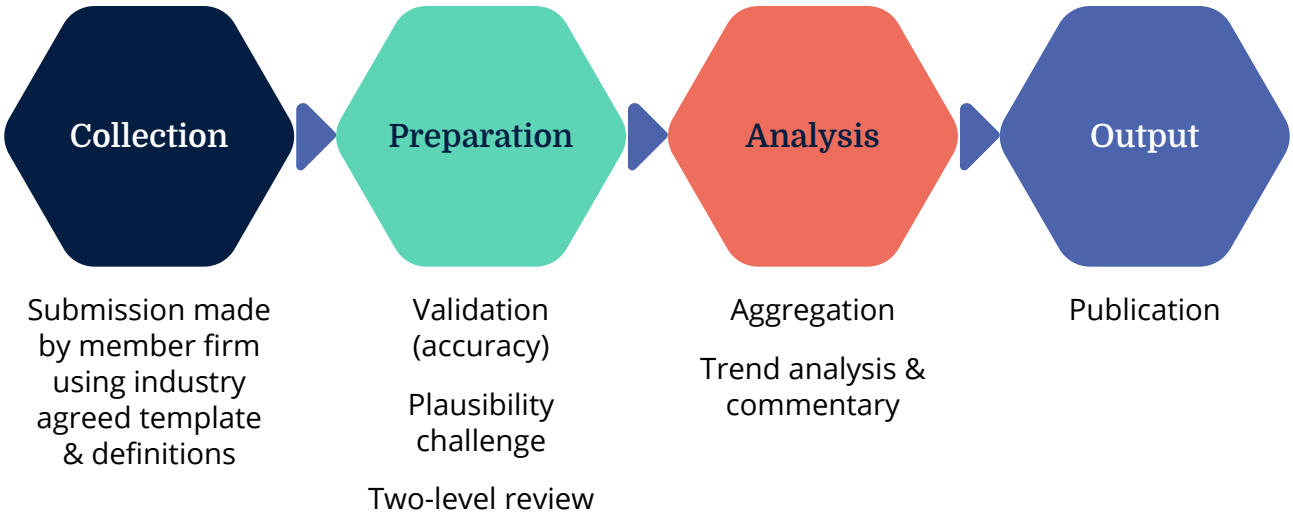
Data plausibility - inputs

Arithmetically correct data for individual members is subject to rangecheck 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.