UK Finance

Annual Fraud Report 2024

In partnership with

feedzai

Table of Contents

About us

Representing 300 firms, 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 financial services industry plays a vital and often underappreciated role enabling individuals, families and communities to achieve their ambitions in a safe and sustainable way – through home ownership, starting a new business or saving for retirement. The sector is fundamental to people's lives, and we are proud to promote the work it is doing to support customers and businesses up and down the country.

Whether it's through innovating for the future, driving economic growth, helping struggling customers amid increases in the cost of living, fighting economic crime or working to finance the net zero transition – the industry is having an overwhelmingly positive effect on the lives of people across the UK and improving the society we live in.

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.

Foreword

We saw some small reductions in the amount stolen through payment fraud in 2023, but with losses of nearly £1.2 billion it remains a major problem and threat to the UK.

The damage this crime does is huge. The organised criminals and other threat actors who perpetrate these awful crimes cause serious harm to individuals, to society and to our country.

Fraud in all its forms continues to represent over 40 per cent of reported crime. That is the scale of the challenge we continue to face.

Moreover, victims often suffer severe emotional damage as fraud is a pernicious and manipulative crime. We see this through the calls our members have with victims, as well as the harrowing case studies we often read about in the media. It is only by stopping fraud happening in the first place that we will truly protect people.

Providing personal and financial data when we make a purchase or register for other online activities has become commonplace. Criminals know this and they focus on compromising personal data to trick customers into making payments or providing enough information to enable a criminal to access and control an account.

This is a process known as social engineering and it is often very sophisticated. It is manipulative and, particularly in some types of crime such as romance fraud, cruel.

The financial services sector spends more than anyone else on combatting economic crime, including fraud. The sector deploys a huge range of sophisticated tools to try and detect potential fraud and enable it to intervene before it happens. Last year, a total of £1.2 billion of unauthorised fraud alone was prevented, an increase of seven per cent.

As new technologies and security systems are deployed it means some routes to defraud individuals have become more difficult, which means criminals shift their tactics and look for other potential weak spots.

The financial sector is at the forefront of efforts to tackle fraud and an important part of this is the wide range of partnerships we have with government departments, regulators, and law enforcement. Intelligence sharing, across both the private and public sector, is a vital tool in disrupting and preventing fraud and there have been major legislative changes recently, such as the Economic Crime and Corporate Transparency Act.

We also fund a specialist police unit, the Dedicated Card and Payment Crime Unit, which is staffed by police officers from the City of London Police and the Metropolitan Police alongside UK Finance colleagues. This unit investigates the criminals responsible and, where possible, brings them to justice.

The best way to tackle fraud is to stop it happening in the first place and our collective efforts should focus on that. Here we have long called for other sectors to step up and stop the criminal activity that is proliferating on their platforms, sites and networks. In 2023, 76 percent of authorised push payment fraud cases originated from online sources and a further 16 per cent from telecommunications. Despite this, these sectors do not have to reimburse victims, nor do they make any contribution via the Economic Crime Levy. We believe it is inequitable for the financial services sector to bear the costs stemming from other sectors' failure to adequately address their own fraud or anti money laundering risks.

There have been some important and welcome improvements, including the government's fraud strategy, the Online Fraud Charter, the Online Safety Act, and good progress by some tech companies. To really move the dial, the commitments made in the Online Fraud Charter need to translate into concrete action across the tech sector. These commitments could also become a global benchmark, building on the UK's fraud summit and recognising the international nature of fraud and the work needed to tackle it.

Ben Donaldson OBE
Managing Director,
Economic Crime,
UK Finance

We have always been clear that reimbursement is important in the fight against fraud. Almost all unauthorised fraud losses are reimbursed and the rate for APP losses increased once again last year.

Later this year there are new rules due to come into force on reimbursement from the Payment Systems Regulator (PSR). The financial services sector is working hard to be ready, but we do have some remaining concerns about the approach being taken by the PSR.

Reimbursement will only ever be part of the solution as victims still suffer and the criminals still get the stolen money.

A cross-sector approach is crucial, as is the sharing of actionable intelligence as well as the delivery of pro-active disruptive measures and operations.

The criminals will always adapt, and fraud will never go away, but by working across sectors to pro-actively suppress the threat, we can help protect the public and make it much harder to commit fraud in the United Kingdom.

The Industry Response:

Representing 300 firms, 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 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 2023 the operational police unit saved the sector and its customers over £33 million, disrupted 10 organised crime groups and secured 68 convictions.
Information & Intelligence (I&I) 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 2023, the I&I Unit disseminated 2,146,381 compromised card numbers enabling card issuers to protect their customers. The unit sent out 427 alerts to the industry and hosted 117 intelligence calls over the year.
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 warning signs that a customer may be falling victim to a scam, before alerting their local police force to intervene and investigate.	The scheme has prevented £312.9m in fraud, engaged with 56,908 emergency calls, and made 1,385 arrests since it launched in 2016. £54.7million of fraud was prevented in 2023.
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. 22 regional police forces, 14 banking brands, and National Trading Standards have signed up to the process.	Over 300 vulnerable people have been referred by law enforcement since the launch in 2023. 50 per cent of vulnerable customers were flagged where the vulnerability was not previously known before the referral was sent in by law enforcement.
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.	There are 39 payment services providers participating in BPS, in 2023 nearly 175,000 cases of APP fraud were created in the system with a combined value of over £300 million, of this £140 million was returned to victims.
Cross sector operations – collaboration with cross sector industries including telecoms, tech companies, and Ofcom to share specific data and intelligence to mitigate live scam attacks.	The blocking of impersonation calls, SMS, high risk advertisements and purchase scam posts remained a core cross sector focus in 2023. The impact of GenAI was also assessed to prevent customers falling victim to large scale social engineering attacks. Over 3,700 unauthorised sender IDs are currently being blocked to prevent them being used to send scam text messages mimicking trusted organisations.
Stakeholder engagement – On behalf of UK Finance members we work with the government, regulators, and all key players in the fraud eco-system to share industry experience and insight, support change and drive the right outcomes for industry and consumers.	Core fraud stakeholder engagement in 2023 related to the delivery of the government's Fraud Strategy, the Online Safety Act, the Economic Crime and Corporate Transparency Act, the new reimbursement requirements from the Payment Systems Regulator (PSR), and the changes needed to PSR rules to enable a risk based approach to payments.
Customer education and awareness campaigns – UK Finance delivers year-round customer education through the 'Take Five to Stop Fraud' campaign, helping people and businesses stay safe 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 to Stop Fraud Charter, bringing the industry together to give people simple and consistent fraud awareness advice. 2023 statistics show seven in ten people recognise an element of the Take Five campaign activity or messaging. Working with education specialists in 2023, UK Finance created a free education resource pack under the Don't Be Fooled Campaign for primary and secondary school pupils to educate and deter them from becoming a money mule. To date 307 schools and ten colleges have signed up to take part.

Foreword from Feedzai

If you worked in fraud prevention last year, you're probably still analysing the shifts and challenges the industry faced. The continued pressure to protect customers from scams, the refinement of new reimbursement regulations, publicly available scam reports, and the emergence of AI into fraud attacks were all significant drivers of change. This perfect storm of factors creates an inflexion point not seen for many years and is forcing the industry to rethink how they protect customers. Understanding user intent is critical, as is ensuring that technology deployed in previous years is still fit for purpose today.

The good news is that efforts applied by UK banks have had a positive impact on fraud. The UK Finance Annual Fraud Report reveals that unauthorised losses were down three per cent in 2023, with Authorised Push Payment (APP) losses also down five per cent. These reductions should be recognised as welcome improvements, but we know there is more to do. A staggering amount of £1.17 billion was still stolen from consumers last year.

Despite a reduction in APP losses, the data reveals that purchase scams were up, whilst impersonation and investment scams were down. The average value of loss in an impersonation scam is £7,448 compared to £549 for a purchase scam, which reflects a change in fraudsters' focus to higher volume, lower value attacks. Separately, romance scams continue to represent the long game for the fraudsters, with an average of ten payments per case (compared to one for purchase scams). The total number of romance scam payments also increased 31 per cent in 2023 and are up 200 per cent from 2020.

The global fraud picture presents an interesting comparison. Unlike in the UK, many countries are experiencing an increase in most types of fraud, especially scams. The US recorded staggering losses of USDf 10 billion[1], and Australia, a country of just 26 million people, recorded AUD 3 billion[2] in APP losses. These figures expose the borderless, relentless nature of financial crime.

The impending Payment Systems Regulator's (PSR) policies are a game-changer. They have the potential to help the most vulnerable amongst us, but will also increase costs for banks. The focus on liability for both sender and receiver will fundamentally reshape how banks manage fraud.

Today, many banks don't monitor mule risk in real-time. Strategies such as the ability to monitor incoming payments will become more common. We already see a convergence of methodologies paving the way for a standardised approach. Focus on the mule also has the potential to disrupt entire criminal networks, exposing individual bad actors and enabling progress in the prevention of broader financial crime. True connectedness between Fraud & AML.

[1]https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public
[2]https://www.accc.gov.au/media-release/accc-calls-for-united-front-as-scammers-steal-over-3bn-from-australians

Whilst the PSR proposal is great for victim protection, unintended consequences could appear. User complacency and increased first party fraud are real possibilities. The UK remains unique in its 100 per cent reimbursement approach; other regions will be closely monitoring progress and using outcomes to influence their own local policies.

Away from scams, there were noticeable takeaways from the data in unauthorised fraud. Card ID theft losses were up 53 per cent compared with 2022 and 200 per cent compared with 2021. This suggests fraudsters are becoming more measured in their approach, by compromising a card identity in a direct channel before making fraudulent transactions on the card.

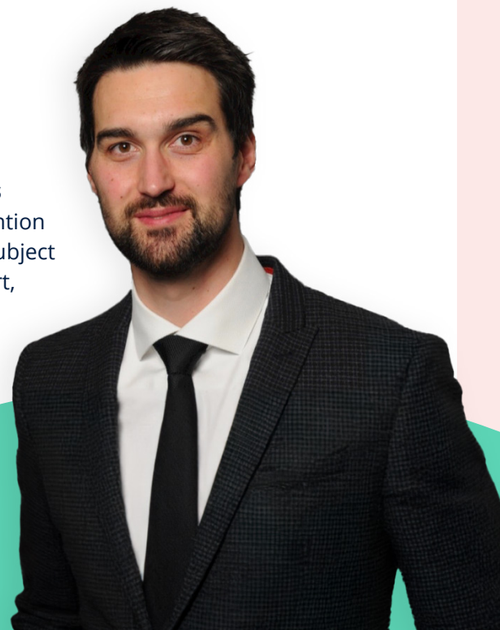
There were interesting movements in the digital fraud space too. Unauthorised losses via web banking were down. The volume of mobile banking cases was up 62 per cent, and for the first time ever, was higher than the volume of web banking cases. The mass adoption of mobile-first banking continues with over 85 per cent of traffic at some tier one institutions coming from mobile. This shift in attack vector likely represents fraudsters recognising that it is difficult to blend into a user's regular behavioural patterns via the web channel.

Underpinning the risk and regulatory landscape we began to see the mainstreaming of GenAI. Imagine fraudsters who already saw an increase in purchase scam success now having access to AI so powerful it can create images, scripts, videos, and voices, in seconds? Two years ago, this wasn't possible. Today, we've all read the headlines of millions lost in a five-minute video call. As fraudster attacks begin to leverage AI, the volume of customers fooled will increase, meaning more fraudulent payments will be processed, therefore fraud rates will increase. It's a natural consequence.

If criminals are using AI, banks must also do so. Having capabilities that allow banks to scale at the same rate as the fraudsters and respond to threats quickly is critical for success. How can GenAI augment fraud detection capability? It could be through operational enhancements and speed of change, as well as detection innovation.

The future requires putting the human factor at the centre of technological innovation and a unified front. The fight against fraud requires adaptability, collaboration, and constant vigilance. Banks cannot fight this battle alone. True disruption requires collaboration across the ecosystem – social giants, tech titans, and telcos must join the fight. Coordinated takedowns and intelligent data exchange are needed to outsmart criminals who operate without borders. Proactive protection of consumers and financial integrity will define the future of security. Anticipating, educating, preventing, and detecting threats is the only way forward.

Feedzai is proud to collaborate with UK Finance for the 2024 Annual Fraud Report. As an industry partner to several UK banks, we're delighted to have this opportunity to share our experience and to reflect on the facts of fraud.



Dan Holmes
Fraud Prevention Strategy & Subject Matter Expert, Feedzai

01

Fraud in 2023

£1.17B
stolen through fraud in 2023

2.97M
confirmed cases

↓4%
on 2022

↓1%
on 2022

£1.2B of unauthorised fraud prevented in 2023, equivalent to 64p in every £1 of attempted

↑7% on 2022

Unauthorised

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

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

	2020	2021	2022	2023	CHANGE
Unauthorised	£783.8m	£730.4m	£726.9m	£708.7m	-3%
Authorised	£420.7m	£583.2m	£485.2m	£459.7m	-5%
Total	**£1204.6m**	**£1313.6m**	**£1212.1m**	**£1168.4m**	**-4%**

Cases

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

	2020	2021	2022	2023	CHANGE
Unauthorised	2,910,509	2,912,467	2,781,311	2,734,934	-2%
Authorised	154,614	195,996	207,372	232,429	12%
Total	**3,065,123**	**3,108,463**	**2,988,683**	**2,967,363**	**-1%**

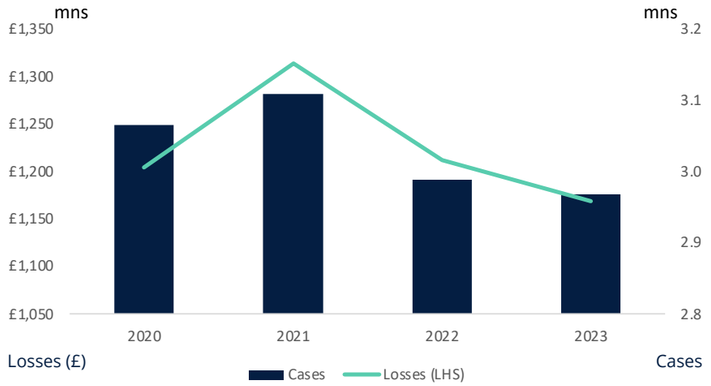
The tide of criminal activity targeting consumers, their means of payment and personal data shows little sign of abating, according to the latest fraud data reported by UK Finance members.

While the sums of money stolen by criminals are vast and the impact on those affected is significant, our data indicates an overall decline in both the value of losses and the number of cases compared with 2022. 2023 marks the second consecutive year of falls on both of these measures.

While the fight to combat fraud has taken some steps in the right direction in the past two years, our detailed breakdown of individual fraud types – across both unauthorised and authorised push payment fraud – point to a continuation of some of the changes we observed in the fraud landscape as we emerged from the pandemic.

In 2023 almost £1.2 billion was lost to fraud. This involved nearly three million cases.

Chart 1 Total fraud losses and case volumes, millions



Source: UK Finance

In this year's report, our data notes trends across a number of fraud types at both ends of the spectrum – some series highs and also series lows – which indicate that the fraud landscape has undergone a material shift in the past few years. Some of this polarisation is a result of changing patterns of consumer behaviour. But additionally, the impact of action taken by industry and regulators is also evident in our data this year.

Table 1 Series records, losses

Series lows	Series highs
Card not received LOWEST SINCE 1991	Lost and stolen HIGHEST SINCE 1991
Remote purchase LOWEST SINCE 2014	Card ID theft HIGHEST SINCE 1991
Internet banking LOWEST SINCE 2014	Authorised purchase scam HIGHEST SINCE 2020*
Authorised investment scam LOWEST SINCE 2020*	Authorised Romance scam HIGHEST SINCE 2020*
	Mobile banking HIGHEST SINCE 2015

* Comparable data on authorised push payment fraud available from 2020

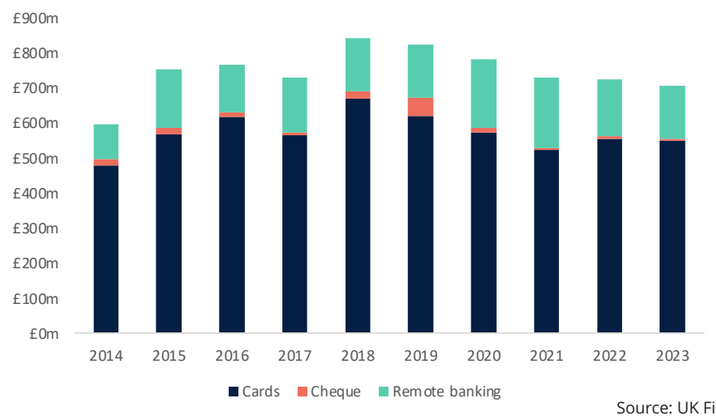
For example, we see further success in reducing some types of fraud, with data pointing to historic lows in the volume of cases and value of certain loss types, for example, card not received fraud.

However, as some routes to defraud individuals become more difficult, criminals have shifted their tactics and this has driven up fraudulent activity in other categories, such as card ID theft and fraud via mobile banking. A recurring theme in this year's data is, once again, this shift towards the compromise of personal data, and social engineering to take over accounts or trick consumers into making payments.

Progress in fraud reduction

Across the two main areas of unauthorised fraud – payment cards and remote banking (unauthorised fraud data also includes cheque fraud, covered in page 34) – 2023 saw a fall in losses compared with 2022. Payment card losses were down one per cent and remote banking losses by seven per cent on 2022. As shown in chart 2, these falls have contributed to the lowest unauthorised fraud losses since 2014, with 2023 losses 16 per cent lower than the peak in 2018.

Chart 2 Authorised fraud losses by category, £ millions



Source: UK Finance

Underneath these encouraging headlines, some diverging trends are in play. One of the main contributors to the overall fall in payment card fraud losses is the nine per cent fall in remote purchase losses in 2023 – the fifth consecutive year of declines in this fraud type, which takes it to the lowest level since 2014. While the drop in 2023 was the largest in our series for this category, remote purchase or card not present fraud still accounts for half of all unauthorised fraud.

Remote purchase fraud relies on criminals acquiring card details through data theft, for example through third party data breaches via phishing emails and scam text messages. Other tactics include 'digital skimming' where card details are compromised when shopping online, either by malicious code on retailers' websites or by tricking consumers with false advertising on social media sites.

Remote purchase losses down 29% in 2023 compared with 2018

The industry has been implementing requirements for Strong Customer Authentication (SCA) to e-commerce over the past two years. This came fully into effect across the industry in March 2022. SCA rules are aimed at reducing fraud by verifying a customer's identity when they make certain higher value online purchases.

The fall in remote purchase losses, particularly in the context of continued growth in online transaction volumes, points to the effectiveness of SCA for consumers relative to static passcodes. However, feedback suggests that it is possible to circumvent these additional protections with criminals using increasingly sophisticated social engineering techniques to trick customers into divulging their one-time passcodes (OTPs) so they can authenticate fraudulent online card transactions.

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.

Also contributing to the overall decline in card losses is the 24 per cent fall in card not received losses in 2023. 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.

Losses and case volumes in this fraud category had been static in the previous three years, but industry feedback suggests that some card issuers have increased the expiry period on cards, thus reducing the volume of cards in transit. This, together with additional activation procedures when cards are received, has contributed to the decline.

Take Five is a national campaign that offers straightforward and impartial advice to help everyone protect themselves from financial fraud. This includes help to spot email deception and phone-based scams as well as online fraud – particularly where criminals impersonate trusted organisations.

Led by UK Finance, the campaign is delivered with and through a range of partners in the UK payments industry, financial services firms, law enforcement agencies, telecommunication providers, commercial, public and third sector organisations.

takefive-stopfraud.org.uk

Changing behaviours and post-pandemic business as usual

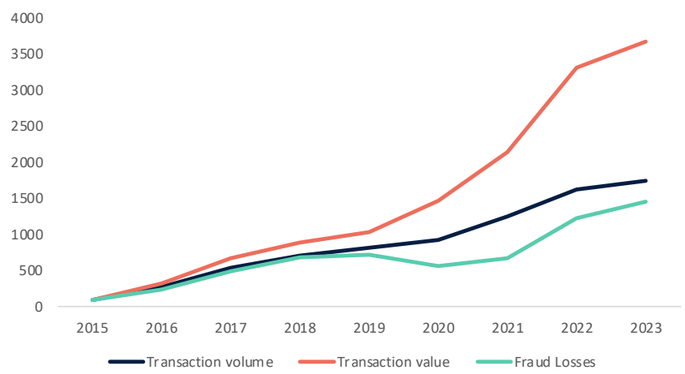
We observed some significant volatility in our data over the pandemic period, from 2020 to 2022, as activities were restricted during lockdowns, payment preferences shifted, and individuals changed the ways in which they access banking services. Some of these responses to the circumstances of the pandemic were enabled and encouraged by the banking and payments industry. Moreover, some of these habits that have stuck with individuals. But this also led the change in tactics adopted by criminals when targeting individuals. Fraud is, in the main, not an opportunistic crime, and criminals continue to evolve their approach as circumstances change.

Our data shows that losses across some fraud types have reverted to pre-pandemic trends, such as internet banking related losses, and lost and stolen card fraud. In other loss categories, data shows the effects of changing preferences and use of technology – for example in the rise in contactless cards and mobile banking losses.

Lost and stolen card losses, which dropped sharply during lockdowns, have returned to pre-pandemic levels in the past two years. This type of 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. This can involve obtaining cards through low-tech methods such as distraction thefts and entrapment devices attached to ATMs.

Related to the rise in lost and stolen fraud is that linked to contactless cards. We called out the growth in contactless card losses in last year's report – in 2022 contactless card losses jumped by over eighty per cent as the limits were increased during the pandemic and there was a significant expansion in acceptance. This rise continued but at a more moderate pace in 2023.

Chart 3 Contactless losses and transactions, 2015=100



Source: UK Finance

However, it is important to put this rise into context (chart 3) – recent rises in contactless fraud have been increasing at a much slower pace than the expansion in transactions volumes and values. The fraud to turnover ratio for contactless fraud, at 1p, remains well below that for unauthorised card fraud overall (5.8p). Contactless cards, therefore, remain a convenient and secure payment method for consumers.

During the pandemic our data showed a rise in internet banking losses. Fraudsters use social engineering through impersonation scam calls or messages to trick individuals into revealing log in details, or remote software applications to take control of online facilities.

As people spent more time at home and online during the pandemic there were more opportunities for criminals to trick people into revealing their security information. As activity normalised in 2022, we saw significant falls in both case volumes and losses – a trend which has continued in our 2023 data. Internet banking losses in 2023 were 22 per cent lower than 2022 and at the lowest level since 2014.

However, the other side of this coin is a further rise in mobile banking related losses, which occurs when bank account details are compromised to gain access to a customer's bank account through a banking app downloaded to a mobile device only. Improvements in functionality and the range of services offered by mobile banking apps have driven a significant increase in adoption. UK Finance's UK Consumer Payments 2023 showed that over 29 million adults used mobile banking, up from 15 million in 2014.

£218m or 59% of attempted Remote banking fraud was prevented.

And with the continued growth in uptake, we have also seen an increase in mobile banking related fraud losses, which rose by a third in 2023, in line with the rate of increase reported in the previous year. Notably, the average loss per case across mobile banking, at £2,270, is lower than the average across all remote banking channels. Banks and individuals may identify suspicious activity sooner rather than later, potentially limiting more significant losses and, importantly, reducing the funds that fall into criminal hands.

Warning lights – fraud risks increasing

The final remote banking channel – telephone banking – had seen a sustained decline in fraud cases and losses in previous years, in line with trends in consumers using this channel. This type of fraud occurs when criminals use compromised bank account details to gain access to a customer's telephone banking account and makes an unauthorised transfer of money away from it. Again, social engineering tactics are used to trick customers into revealing security details, which are used to convince the telephone banking operator they are the account holder.

In 2023 we saw both cases and losses increase by around a fifth – the first increase in four years. Despite the rise, telephone banking losses account for 12 per cent of remote banking losses.

While the industry remains vigilant for indications that artificial intelligence (AI), including voice cloning, is being adopted by criminals to compromise back accounts, feedback suggests that this has not been identified as a driver behind the rise in telephone banking losses. However, the implications of AI in the fraud landscape are being closely monitored across the industry.

The most significant area of growth across all our fraud categories is card ID theft. In 2023 losses were 53 per cent higher than in 2022 and cases rose by 74 per cent. This followed a near-doubling in case volumes and losses in 2022. 2023 data represent the highest ever recorded. In 2023 card ID theft accounted for 14 per cent of all payment card losses, up from seven per cent in 2018.

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 (more details on this breakdown can be found in the next section).

Underpinning this type of fraud is the compromise of personal data – this can be via phishing emails, scam messages, data scraped from social media sites, and information physically stolen from mailboxes. Providing our personal data when we make a purchase or register for other online activities has become commonplace, but when this finds its way into the wrong hands it can enable criminals to takeover an account or to make a fake application.

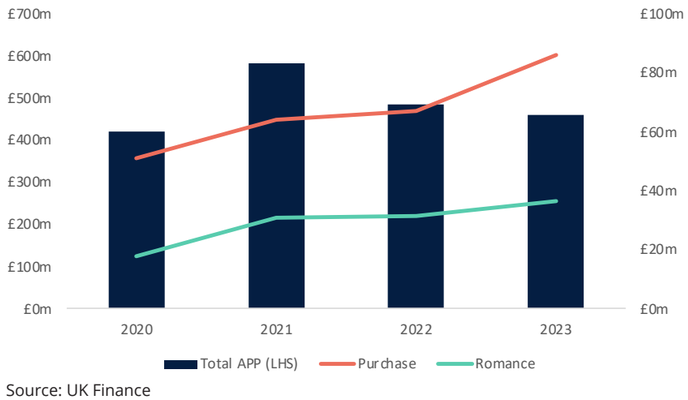
The growth in this type of fraud marks a shift away from criminals seeking to target systems and infrastructure, to tactics which see the individual as the weakest link to exploit. The rise in card ID theft in the past two year also nearly offsets the progress made in reducing remote purchase fraud through SCA. Moreover, the average loss per case through card ID theft is more than three times that of remote purchase.

The industry continues to invest in technology that can help identify and flag potentially fraudulent activity, as well as raising awareness amongst customers about how they can manage personal data security. However, the data suggests that investment in technology that monitors transactions and can identify unusual customer behaviour that may indicate potentially fraudulent activity can only go so far. Where prevention is within the control of banks or payment providers, progress on fraud reduction has been tangible in recent years, reinforcing the need for consumer education and collaboration with other stakeholders and agencies.

Moving from unauthorised to authorised push payment (APP) fraud for the final two areas of increase to call out in this year's report. As chart 4 illustrates, the total value of APP losses have fallen from their pandemic peaks, with a drop of five per cent in 2023. However, within this case numbers continue to grow, increasing 12 per cent in 2023 compared with the previous year.

Two categories within APP fraud are almost entirely responsible for the growth in cases – romance and purchase scams. Chart 4 also shows that losses rose by 17 per cent and 28 per cent respectively in 2023.

Chart 4 APP fraud losses, £ million



Source: UK Finance

In romance scams victims are persuaded to make payments to a person they have met, often online, 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. The damage done by these scams often goes beyond the financial and into significant emotional harm. 2023 saw another year of increase in both case and losses related to these scams, with losses twice the level of those reported in 2020.

Romance scams involve an average of nearly ten payments per case

Given the long-term nature of some of these cases, which involve an average of nearly ten separate payments per case, it is likely that many of these fraud events pre-date 2023 and have only now come to light. One of the factors that romance fraud has in common with purchase scams is where the fraud originates.

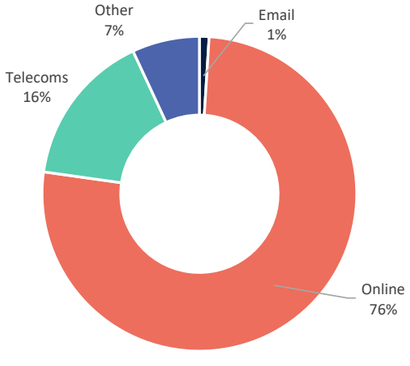
UK Finance data shows that over three-quarters of APP fraud cases originate online (chart 5), a figure consistent with the one we reported for 2022. These types of fraud, like the compromise of data in some unauthorised fraud types, work by targeting individuals rather than systems or institutions.

More significant growth in the APP fraud categories is seen in purchase scams, where the scale of losses is second only to investment scams in the authorised category and have overtaken impersonation (bank or police) scams. In a purchase scam, the victim pays in advance for goods or services that are never received, usually ordered on an online platform such as an auction website or social media.

Many online platforms offer secure payment options, but fraudsters convince the victim to pay via a bank transfer instead. It is perhaps assumed that purchase scams only involve high volumes of lower value 'too good to be true' scams. However, data provided by Voluntary Code members , point to around nine per cent of cases and two-thirds of losses involving purchases with a value in excess of £1,000.

Working with the online platforms that are used to defraud consumers is the most effective route to tackling these types of scams. Recent moves to more robust seller verification on online auction sites is an example of the impact of industry engagement with online platforms, but there remains more to be done to close down the opportunities for fraudsters to use their systems.

Chart 5 APP fraud origination, percentage of total



Source: UK Finance

One area of APP fraud to watch in the coming year is the evolution of losses across investment scams – the largest loss category in authorised fraud. In 2023 losses through investment scams dropped by five per cent, following a more significant 34 per cent fall in 2022. Declines over the past two years may reflect the cost-of-living challenges that have affected almost all household budgets in recent years and made individuals more cautious with their constrained finances. As these pressures are expected to dissipate in 2024 with rising real incomes, the risk of losses through investment scams could increase. In addition, recent increases in cryptocurrency prices, which have received a lot of coverage in mainstream and social media, could be exploited by criminals to trick potential victims with the promise to big returns on investments.

Prevention and reimbursement

Our report focuses on the scale and nature of losses through payment fraud. This information can inform industry and policy makers as well as help alert the public about the evolving nature of threats in the fraud landscape. In addition, our data also captures the financial impact of fraud prevention, and the value of funds reimbursed and repatriated to victims.

A pound value on prevented fraud can only be attributed to unauthorised fraud as it isn't possible to fully quantify APP fraud that is captured earlier in the payment journey, for example systems will not capture an individual abandoning a payment as a result of effective warning messages. The banking and payments industry has been calling for action to enable a more risk-based approach to payments giving firms additional time to investigate certain suspicious transactions. The recent announcement from the government to enable certain payments to be slowed could make a material difference, particularly to larger value fraudulent transactions.

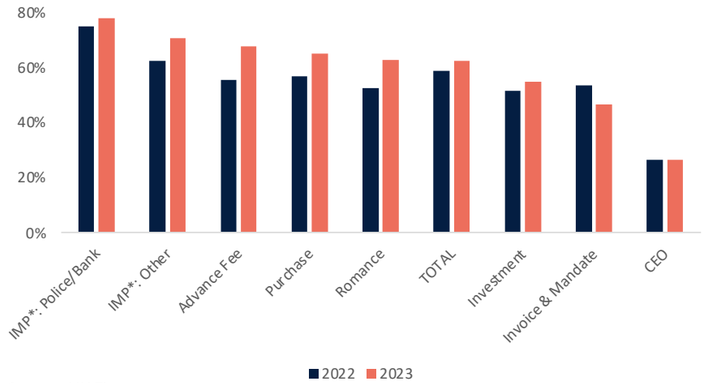
In 2023 £1.2 billion of unauthorised fraud was prevented – a seven per cent increase on 2022 and equal to 64p in every £1 of fraud attempted. A rise in the value of prevented fraud was recorded across the two main authorised categories, with a four per cent increase in prevented payment card fraud and a 25 per cent increase in remote banking fraud prevention. This highlights the ongoing efforts from industry to reduce harm to consumers and prevent money from reaching criminals in the face of an ever-evolving fraud landscape.

In addition to prevention, bank and payments providers also have responsibilities for reimbursement to victims of fraud. Unauthorised fraud, where the victim has no knowledge of the activity, is generally fully returned to the affected individual. UK Finance research has shown that over 98 per cent of unauthorised fraud losses are returned to the victim.

Reimbursement for APP fraud is more complex as it involves victims unwittingly initiating the payment. Reimbursements rates rose across almost all categories of APP fraud in 2023 (chart 6), with a total of 62 per cent of all APP losses returned to victims, up from 59 per cent in 2022 and 45 per cent in 2020. These rates will continue to rise following consultation from the Payment Systems Regulator (PSR) on mandatory reimbursement, which will come into play later this year.

This offers individuals some reassurance that, if they are targeted by criminals in this type of fraudulent activity, they will not ultimately be out of pocket. However, it is still important for individuals to take the necessary precautions when engaging with certain types of transaction initiated over the telephone and online. Consumer awareness-raising – such as the UK Finance-led Take Five to Stop Fraud campaign – will continue to be critical in highlighting the potential risks from fraud and scams. Online platforms and telecoms companies, while not in scope as part of the reimbursement process are, as illustrated above, where APP fraud originates. These companies must also play their part to crack down on funds flowing into criminal hands.

Chart 6 APP reimbursement rates, percentage



Source: UK Finance

* Impersonation

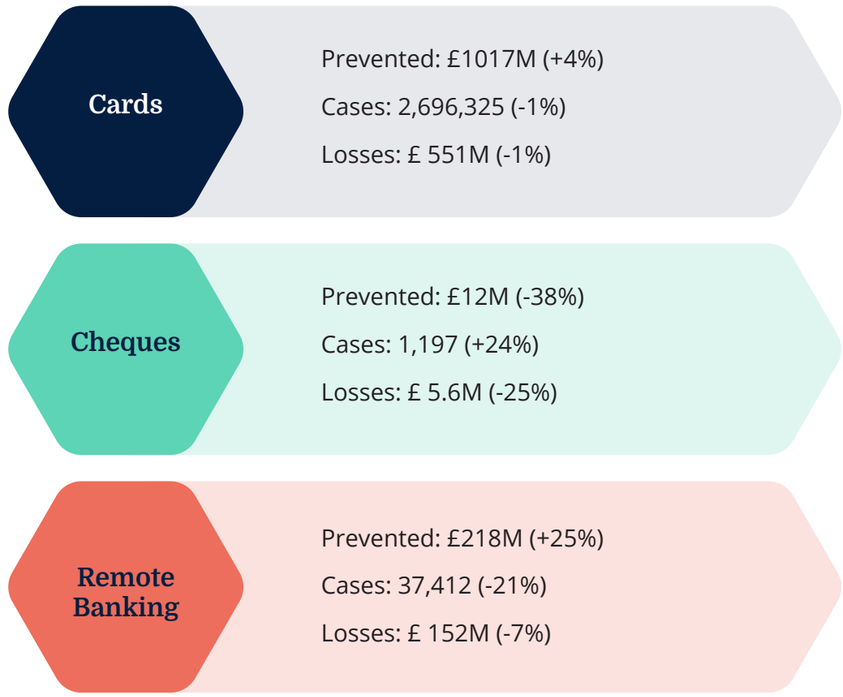
The remainder of this report will outline the complete data set across all fraud types, noting headline trends and drivers for each fraud category.

02

Unauthorised Fraud Summary

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

- Unauthorised fraud losses were **£708.7 million** in 2023, **down three per cent** on 2022.
- There were **2.7 million** cases of unauthorised fraud, **two per cent lower** than in 2022.
- The industry prevented a further **£1.247 billion** of unauthorised fraud – equivalent to 64p in every £1 of attempted unauthorised fraud being stopped without a loss occuring.



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 £551.3 million in 2023, a one per cent fall from £556.3 million in 2022.

Card fraud losses and cases fell by

1%

in 2023 compared than 2022.

Fraud to turnover for card fraud overall (excluding cash acquisition) totalled

5.8p

in 2023, down from 6.0 pence in 2022

£1B

of card fraud prevented

+4%

on 2022.

Losses

Total value of gross losses -

VALUES	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	CHANGE
Prevented	N/A	£843.5m	£986.0m	£984.8m	£1126.4m	£1007.5m	£983.4m	£966.6m	£974.2m	£1016.5m	4%
Lost & stolen	£59.7m	£74.1m	£96.3m	£92.9m	£95.1m	£94.8m	£78.9m	£77.2m	£100.2m	£104.0m	4%
CNR	£10.1m	£11.7m	£12.5m	£10.2m	£6.3m	£5.2m	£4.4m	£3.9m	£4.0m	£3.0m	-24%
Counterfeit	£47.8m	£45.7m	£36.9m	£24.2m	£16.3m	£12.8m	£8.7m	£4.7m	£4.7m	£4.7m	0%
Remote purchase	£331.5m	£398.4m	£432.3m	£408.4m	£506.4m	£470.2m	£452.6m	£412.5m	£395.7m	£360.5m	-9%
Card ID Theft	£30.0m	£38.2m	£40.0m	£29.8m	£47.3m	£37.7m	£29.7m	£26.3m	£51.7m	£79.1m	53%
Total	**£479.0m**	**£568.1m**	**£618.1m**	**£565.4m**	**£671.4m**	**£620.6m**	**£574.2m**	**£524.5m**	**£556.3m**	**£551.3m**	**-1%**
UK fraud	£328.7m	£379.7m	£417.9m	£407.5m	£496.6m	£449.9m	£414.5m	£384.0m	£416.2m	£416.8m	0%
International fraud	£150.3m	£188.4m	£200.1m	£158.0m	£174.8m	£170.7m	£159.7m	£140.5m	£140.1m	£134.5m	-4%

Cases

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

CASES	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	CHANGE
Lost & stolen	133,943	143,802	231,164	350,279	434,991	460,142	321,994	325,501	401,340	397,549	-1%
CNR	9,302	10,719	11,377	10,903	10,046	7,907	8,435	8,941	8,848	5,933	-33%
Counterfeit	99,279	86,021	108,597	85,025	58,636	65,907	52,782	24,908	19,594	18,070	-8%
Remote purchase	1,019,146	1,113,084	1,437,832	1,398,153	2,050,275	2,157,418	2,417,866	2,425,099	2,221,026	2,132,331	-4%
Card ID Theft	26,542	33,566	31,756	29,156	63,791	54,165	34,545	38,753	82,064	142,442	74%
Total	**1,288,212**	**1,387,192**	**1,820,726**	**1,873,516**	**2,617,739**	**2,745,539**	**2,835,622**	**2,823,202**	**2,732,872**	**2,696,325**	**-1%**

Analysis by Unauthorised Card Fraud Case Type

Lost and Stolen Card Fraud

Value • £104.0m (4%) **Cases** • 397,549 (-1%)

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.

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	CHANGE
Value	£59.7m	£74.1m	£96.3m	£92.9m	£95.1m	£94.8m	£78.9m	£77.2m	£100.2m	£104.0m	4%
Cases	133,943	143,802	231,164	350,279	434,991	460,142	321,994	325,501	401,340	397,549	-1%

- Loss total of £104 million is the highest ever reported
- One third of all lost & stolen fraud spend is contactless

Card not received

Value • £3.0m (-24%) **Cases** • 5,933 (-33%)

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.

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	CHANGE
Value	£10.1m	£11.7m	£12.5m	£10.2m	£6.3m	£5.2m	£4.4m	£3.9m	£4.0m	£3.0m	-24%
Cases	9,302	10,719	11,377	10,903	10,046	7,907	8,435	8,941	8,848	5,933	-33%

- Lowest totals ever reported for both loss and case volume
- Industry feedback suggests that some card issuers have increased the expiry period on cards, thus reducing the volume of cards in transit. This, together with additional activation procedures when cards are received have caused the decline.

Counterfeit Card Fraud

Value • £4.7m (0%) **Cases** • 18,070 (-8%)

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

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	CHANGE
Value	£47.8m	£45.7m	£36.9m	£24.2m	£16.3m	£12.8m	£8.7m	£4.7m	£4.7m	£4.7m	0%
Cases	99,279	86,021	108,597	85,025	58,636	65,907	52,782	24,908	19,594	18,070	-8%

- Lowest total ever reported for case volume
- Losses unchanged in the past three years
- Fraud spends restricted to those countries which do not utilise chip & PIN technology.

Remote Purchase (CNP) Fraud

Value • £360.5m (-9%) **Cases** • 2,132,331 (-4%)

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

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	CHANGE
Value	£331.5m	£398.4m	£432.3m	£408.4m	£506.4m	£470.2m	£452.6m	£412.5m	£395.7m	£360.5m	-9%
Cases	1,019,146	1,113,084	1,437,832	1,398,153	2,050,275	2,157,418	2,417,866	2,425,099	2,221,026	2,132,331	-4%

- Loss total of £360.5 million is the lowest reported for 9 years (2014)
- Lowest case volume total reported for 5 years (2018)
- In March 2022, requirements for Strong Customer Authentication (SCA) in the context of e-commerce took effect. SCA rules are aimed at reducing fraud by verifying a customer's identity when they make certain higher value online purchases. The new rules have reduced by not eliminated this fraud type as criminals still try to circumvent these additional protections by tricking customers into divulging their one-time passcodes (OTPs).

SCA introduction

Card ID Theft

Value • £79.1m (+53%) Cases • 142,442 (+74%)

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 • £31.7m (+84%) Cases • 20,792 (+25%)

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 • £47.4m (+37%) Cases • 121,650 (+85%)

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

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	CHANGE
Value	£30.0m	£38.2m	£40.0m	£29.8m	£47.3m	£37.7m	£29.7m	£26.3m	£51.7m	£79.1m	53%
Cases	26,542	33,566	31,756	29,156	63,791	54,165	34,545	38,753	82,064	142,442	74%

- Loss total is the highest ever reported
- Case volume total is the highest ever reported
- Compromise of personal data continues to drive both types of Card ID theft.
- Account takeover fraud, although difficult to commit, has become more attractive after the changes introduced as part of SCA, specifically OTP's change the criminal's behaviour – the possibility of gaining access to a customers' existing accounts, changing personal details, and reordering replacement cards is potentially more lucrative than social engineering one OTP from a victim directly.

Further Card Fraud Analysis

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 • £91.4m (+23%)

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.

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	CHANGE
Value	£49.3m	£53.5m	£62.8m	£61.9m	£69.8m	£64.3m	£48.9m	£48.3m	£74.4m	£91.4m	23%

- Fraudulent contactless spend totalled £41.5 million in 2023; an increase of 19 per cent on 2022; the highest total reported for this category since it was introduced in 2014
- Recent rises in contactless fraud have been increasing at a much slower pace than the expansion in transactions volumes and values, and the fraud to turnover ratio for contactless fraud remains below that for unauthorised card fraud overall. Contactless cards, therefore, remain a convenient and secure payment method for consumers.
- Contactless fraud on payment cards and devices represents only eight per cent of overall card fraud losses, while 73 per cent of all card transactions were contactless last year.

UK Internet / e-commerce Card Fraud Losses

Value • £260.0m (-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.

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	CHANGE
Value	£190.1m	£219.1m	£261.5m	£310.3m	£310.4m	£360.5m	£377.2m	£339.2m	£285.2m	£260.0m	-9%

- Loss total is the lowest reported for 9 years (2014)
- 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.

UK Cash Machine Fraud Losses

Value • £25.6m (-2%)

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.

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	CHANGE
Value	£27.3m	£32.7m	£43.1m	£37.2m	£32.6m	£30.0m	£28.1m	£24.4m	£26.1m	£25.6m	-2%

Card Fraud Abroad

Value • £134.5m (-4%)

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

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	CHANGE
Value	£150.3m	£188.4m	£200.1m	£158.0m	£174.8m	£170.7m	£159.7m	£140.5m	£140.1m	£134.5m	-4%

04

Unauthorised Cheque Fraud

Overall Cheque Fraud

Value • £5.6m (-25%) Cases • 1,197 (+24%)

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	CHANGE
Prevented	N/A	£392.8m	£196.2m	£212.3m	£218.2m	£550.8m	£238.5m	£33.1m	£19.8m	£12.3m	-38%
Value	£20.2m	£18.9m	£13.7m	£9.8m	£20.6m	£53.6m	£12.3m	£6.4m	£7.5m	£5.6m	-25%
Cases	8,168	5,746	3,388	1,745	2,020	2,852	1,247	815	966	1,197	24%

- Cheque fraud accounts for less than one per cent of all unauthorised fraud
- Lowest loss total ever reported
- Lowest prevented cheque fraud total ever reported (£12.3 million)
- Overall prevention rate for cheque fraud was 69 per cent in 2023

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

Counterfeit cheque fraud

Value • £1.0m (-44%) Cases • 483 (+132%)

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 • £3.1m (-6%) Cases • 513 (+45%)

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 (-38%) Cases • 201 (-50%)

A forged cheque is a genuine cheque that has been stolen from an innocent customer and used by a fraudster with a forged signature. customers' existing accounts, changing personal details, and reordering replacement cards is potentially more lucrative than social engineering one OTP from a victim directly.

05

Unauthorised Remote Banking Fraud

Overall Unauthorised remote banking fraud

Value • £151.8m (-7%) Cases • 37,412 (-21%)

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.

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	CHANGE
Prevented	N/A	£524.6m	£205.4m	£261.1m	£317.7m	£268.9m	£393.8m	£365.5m	£174.1m	£218.1m	25%
Value	£98.2m	£168.6m	£137.0m	£156.1m	£152.9m	£150.7m	£197.3m	£199.5m	£163.1m	£151.8m	-7%
Cases	21,819	33,306	33,392	34,746	31,797	43,920	73,640	88,450	47,473	37,412	-21%

- In 2023, nearly nine in ten of the adult population used at least one form of remote banking
- Overall prevention rate for remote banking fraud was 59 per cent in 2023
- For the first time the confirmed number of mobile banking cases exceeds internet banking confirmed cases

There are three types of remote banking fraud: Internet, telephone and mobile banking

Unauthorised Internet Banking Fraud

Value • £88.7m (-22%) Cases • 13,669 (-57%)

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.

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	CHANGE
Value	£81.4m	£133.5m	£101.8m	£121.2m	£123.0m	£111.8m	£159.7m	£158.3m	£114.1m	£88.7m	-22%
Cases	16,041	19,691	20,088	21,745	20,904	25,849	55,995	72,557	32,036	13,669	-57%

- Lowest loss total reported since 2014
- Lowest case volume total since 2012
- Internet banking losses in 2023 were 45 per cent down on the peak reported during Covid-19 lockdown in 2020 (£159.7 million)
- The reduction, in part reflects, the fall in the proportion of adults using internet banking in the past two years and the migration to mobile banking apps
- A further £20 million was recovered after the incident occurred

Unauthorised Telephone Banking Fraud

Value • £17.6m (+19%) Cases • 3,711 (+21%)

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

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	CHANGE
Value	£16.8m	£32.3m	£29.6m	£28.4m	£22.0m	£23.6m	£16.1m	£15.5m	£14.7m	£17.6m	19%
Cases	5,778	11,380	10,495	9,577	7,937	11,199	7,490	4,623	3,076	3,711	21%

- 2023 is the first time both losses and case volumes have increased since 2019
- 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.
- £29.7 million of telephone banking fraud was prevented in 2023, equivalent to £6.27 in every £10 of attempted fraud being stopped without a loss occurring.
- A further £1.4 million was recovered after the incident had occurred.

Unauthorised Mobile Banking Fraud

Value • £45.5m (+33%) **Cases** • 20,032 (+62%)

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).

	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	CHANGE
Value	N/A	£2.8m	£5.7m	£6.5m	£7.9m	£15.2m	£21.6m	£25.8m	£34.2m	£45.5m	33%
Cases	N/A	2,235	2,809	3,424	2,956	6,872	10,155	11,270	12,361	20,032	62%

*Mobile banking losses were not collected prior to 2015.

- Loss total highest ever reported
- Case volume total highest ever reported
- 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.
- £48.5 million of telephone banking fraud was prevented in 2023, equivalent to 52p in every £1 of attempted fraud being stopped without a loss occurring.
- A further £3.0 million was recovered after the incident had occurred.

06

Authorised Payment Fraud

Authorised push payment fraud

Value • £459.7m (-5%) Cases • 232,429 (+12%)

Authorised push payment (APP) fraud occurs when a victim is tricked into sending money directly from their account to an account which controlled by a fraudster.

APP fraud losses continue to be driven by the abuse of online platforms used by criminals to scam their victims. These include investment scams advertised on search engines and social media, romance scams committed via online dating platforms and purchase scams promoted through auction websites.

Once the victim has authorised the payment and the money has reached the criminal's account, the criminal will quickly transfer the money out to numerous other accounts, often abroad, where it is then cashed out.

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

Cases

232,429 (+12%)

Highest total recorded (2020)
Purchase scam 67% of all cases
All case type decreased except; Purchase romance and Investment scams

Losses

£459.7M (-5%)

All case types decreased except: Purchase, (highest recorded), romance (highest recorded) and invoice and mandate

Reimbursement

£287.3M (+1%)

62% of all APP losses returned to victims in 2023, up from 59% in 2022 or 45% in 2020

		2020	2021	2022	2023	CHANGE
Cases	Personal	145,207	188,964	200,643	224,694	12%
	Non-Personal	9,407	7,032	6,729	7,735	15%
	Total	**154,614**	**195,996**	**207,372**	**232,429**	**12%**
Payments	Personal	228,946	333,751	361,761	405,095	12%
	Non-Personal	15,625	11,386	10,505	12,364	18%
	Total	**244,571**	**345,137**	**372,266**	**417,459**	**12%**
Value	Personal	£347.4m	£505.9m	£408.2m	£376.4m	-8%
	Non-Personal	£73.3m	£77.4m	£77.0m	£83.3m	8%
	Total	**£420.7m**	**£583.2m**	**£485.2m**	**£459.7m**	**-5%**
Returned to victim	Personal	£163.4m	£246.8m	£254.1m	£256.4m	1%
	Non-Personal	£27.4m	£24.4m	£31.5m	£30.8m	-2%
	Total	**£190.8m**	**£271.2m**	**£285.6m**	**£287.3m**	**1%**

07

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 scams 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 is able to provide data which shows the sources of Authorised Push Payment fraud (APP). We can do this through analysis of a subset of APP data which uses anonymised case data that includes insight on the reported origination of fraud events.

	2022		2023	
	VOLUME	VALUE	VOLUME	VALUE
Online	78%	36%	76%	30%
Telecommunications	18%	45%	16%	43%
Email	2%	12%	1%	11%
Other	2%	7%	7%	16%

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.
- Data may be subject to future restatement if further information becomes available.

This shows that

76% of fraud cases originate from online sources. These cases tend to include lower-value scams such as purchase fraud and therefore account for **30%** of total losses

16% of fraud cases originate from telecommunications, these are usually higher value cases such as impersonation scams and so account for **43%** of total losses

08

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 provides protections for customers of signatory payment service providers (PSPs) and delivers a significant commitment from all signatory firms to reimburse victims of APP 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.

In 2023, 214,344 cases were assessed and closed with a total value of £351.0 million. Our latest figures show that £256.5 million of losses were returned to victims under the APP voluntary code, accounting for 73 % of losses in these cases.

	<£1k	>£1k <£10k	>£10k	Total
Cases	174,582	33,994	5,768	214,344
Payments	245,145	93,308	46,707	385,160
Value	£40.5m	£102.4m	£208.1m	£351.0m
Returned to victim	£30.8m	£65.5m	£144.2m	£256.5m*

* This includes £15.9m 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

09

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.

Purchase Scam

Value • £85.9m (+28%) **Cases** • 156,516 (+34%)

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 2020-2023

		2020	2021	2022	2023	CHANGE
Cases	Personal	80,214	97,382	114,417	152,837	34%
	Non-Personal	4,078	2,351	2,753	3,679	34%
	Total	**84,292**	**99,733**	**117,170**	**156,516**	**34%**
Payments	Personal	102,325	129,442	155,451	214,690	38%
	Non-Personal	5,168	2,969	3,667	4,904	34%
	Total	**107,493**	**132,411**	**159,118**	**219,594**	**38%**
Value	Personal	£44.7m	£56.8m	£59.6m	£77.0m	29%
	Non-Personal	£6.5m	£7.4m	£7.4m	£8.9m	21%
	Total	**£51.1m**	**£64.1m**	**£67.0m**	**£85.9m**	**28%**
Returned to victim	Personal	£14.2m	£20.0m	£35.3m	£51.6m	46%
	Non-Personal	£1.7m	£2.1m	£2.8m	£4.2m	49%
	Total	**£15.9m**	**£22.1m**	**£38.1m**	**£55.8m**	**46%**

- Loss total highest ever recorded
- Case total highest ever recorded
- 67 per cent of all APP scams reported in 2023 were purchase scams accounting for 19 per cent of the value
- The reimbursement rate in 2023 was 65 per cent, up from 31 per cent in 2020.
- 92 per cent of purchase scams originate 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.

	<£1k	>£1k <£10k	>£10k	Total
Cases	133,130	12,674	696	146,500
Payments	176,475	26,369	3,196	206,040
Value	£25.5m	£36.1m	£15.2m	£76.8m
Returned to victim	£19.5m	£20.5m	£9.6m	£49.6m

- 65 per cent of all losses were returned to the victim in 2023 compared with 34 per cent in 2021
- 91 per cent of all cases assessed involved case values of less than £1,000

Investment Scam

Value • £107.8m (-5%) **Cases** • 10,226 (+1%)

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 2020-2023

		2020	2021	2022	2023	CHANGE
Cases	Personal	7,900	11,905	9,941	10,060	1%
	Non-Personal	281	169	144	166	15%
	Total	**8,181**	**12,074**	**10,085**	**10,226**	**1%**
Payments	Personal	19,322	35,071	30,065	32,780	9%
	Non-Personal	601	594	446	616	38%
	Total	**19,923**	**35,665**	**30,511**	**33,396**	**9%**
Value	Personal	£103.6m	£166.2m	£109.3m	£98.6m	-10%
	Non-Personal	£5.8m	£5.5m	£4.8m	£9.3m	94%
	Total	**£109.4m**	**£171.7m**	**£114.1m**	**£107.8m**	**-5%**
Returned to victim	Personal	£39.0m	£72.7m	£56.9m	£56.3m	-1%
	Non-Personal	£1.2m	£2.0m	£1.7m	£2.7m	61%
	Total	**£40.2m**	**£74.6m**	**£58.6m**	**£59.0m**	**1%**

- Lowest loss total ever recorded; however, it still accounts for largest proportion of the eight scam types for loss; accounting for 23 per cent of all APP losses reported in 2023
- A driver behind the reduction is the emergence of cost-of-living pressures, individuals are more cautious with money and less likely to be looking for investment opportunities and therefore less likely to encounter a fraudulent investment opportunity
- The reimbursement rate in 2023 was 55 per cent, up from 37 per cent in 2020
- 68 per cent of investment scams originated online in 2023

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.

	<£1k	>£1k <£10k	>£10k	TOTAL
Cases	4,746	2,374	1,439	8,559
Payments	8,461	9,432	10,691	28,584
Value	£1.6m	£8.7m	£66.5m	£76.7m
Returned to victim	£1.0m	£4.9m	£41.1m	£47.1m

- 61 per cent of all losses were returned to the victim in 2023 compared with 45 per cent in 2021

Romance Scam

Value • £36.5m (+17%) **Cases** • 4,160 (+14%)

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 – 2023

		2020	2021	2022	2023	CHANGE
Cases	Personal	2,252	3,245	3,617	4,134	14%
	Non-Personal	73	25	32	26	-19%
	Total	**2,325**	**3,270**	**3,649**	**4,160**	**14%**
Payments	Personal	12,778	25,723	30,119	39,395	31%
	Non-Personal	407	91	101	183	81%
	Total	**13,185**	**25,814**	**30,220**	**39,578**	**31%**
Value	Personal	£17.3m	£30.6m	£30.9m	£36.1m	17%
	Non-Personal	£0.5m	£0.3m	£0.4m	£0.4m	-4%
	Total	**£17.8m**	**£30.9m**	**£31.3m**	**£36.5m**	**17%**
Returned to victim	Personal	£6.5m	£12.4m	£16.3m	£22.6m	39%
	Non-Personal	£0.1m	£0.2m	£0.2m	£0.3m	69%
	Total	**£6.6m**	**£12.6m**	**£16.4m**	**£22.9m**	**39%**

- Highest loss total ever reported
- Highest case volume total ever reported
- Romance scams have an average of nearly ten 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
- The reimbursement rate in 2023 was 63 per cent, up from 37 per cent in 2020.
- 84 per cent of all Romance scams originated online in 2023

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 purchase scam cases reported and should not be treated as an addition.

	<£1k	>£1k <£10k	>£10k	Total
Cases	1,795	1,318	576	3,689
Payments	6,047	13,733	16,472	36,252
Value	£0.6m	£4.7m	£24.3m	£29.6m
Returned to victim	£0.5m	£3.2m	£15.9m	£19.6m

- 66 per cent of all losses were returned to the victim in 2023 compared with 44 per cent in 2021

Advance Fee Scam

Value • £31.3m (-3%) **Cases** • 23,849 (-13%)

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 2020-2023

		2020	2021	2022	2023	CHANGE
Cases	Personal	13,316	19,950	26,871	23,526	-12%
	Non-Personal	517	545	458	323	-29%
	Total	**13,833**	**20,495**	**27,329**	**23,849**	**-13%**
Payments	Personal	22,434	36,166	50,463	50,223	-0%
	Non-Personal	798	804	768	737	-4%
	Total	**23,232**	**36,970**	**51,231**	**50,960**	**-1%**
Value	Personal	£21.2m	£30.8m	£30.7m	£29.4m	-4%
	Non-Personal	£1.0m	£1.4m	£1.5m	£2.0m	32%
	Total	**£22.2m**	**£32.1m**	**£32.2m**	**£31.3m**	**-3%**
Returned to victim	Personal	£7.4m	£10.9m	£17.2m	£20.4m	19%
	Non-Personal	£0.3m	£0.9m	£0.6m	£0.8m	32%
	Total	**£7.7m**	**£11.8m**	**£17.8m**	**£21.2m**	**19%**

- Cases and losses fell 13 per cent and three per cent respectively in 2023 compared with 2022
- The reimbursement rate in 2023 was 68 per cent, up from 35 per cent in 2020
- Deposits for high value goods remain a key driver behind this scam type
- 65 per cent of advance fee scams originated online in 2023

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 purchase scam cases reported and should not be treated as an addition.

	<£1k	>£1k <£10k	>£10k	Total
Cases	18,693	3,056	429	22,178
Payments	31,964	10,642	5,079	47,685
Value	£4.6m	£8.1m	£14.5m	£27.2m
Returned to victim	£3.7m	£4.9m	£9.8m	£18.4m

- 67 per cent of all losses were returned to the victim in 2023 compared with 34 per cent in 2021

Invoice & Mandate Scam

Value • £50.3m (+2%) **Cases** • 3,110 (-7%)

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 2020-2023

		2020	2021	2022	2023	CHANGE
Cases	Personal	2,903	2,555	1,871	1,485	-21%
	Non-Personal	1,818	1,775	1,469	1,625	11%
	Total	**4,721**	**4,330**	**3,340**	**3,110**	**-7%**
Payments	Personal	3,904	3,676	2,836	2,176	-23%
	Non-Personal	2,416	2,491	2,129	2,233	5%
	Total	**6,320**	**6,167**	**4,965**	**4,409**	**-11%**
Value	Personal	£25.1m	£19.9m	£15.0m	£15.3m	2%
	Non-Personal	£43.6m	£36.8m	£34.5m	£35.0m	2%
	Total	**£68.8m**	**£56.7m**	**£49.5m**	**£50.3m**	**2%**
Returned to victim	Personal	£15.7m	£12.6m	£12.4m	£12.4m	0%
	Non-Personal	£16.1m	£10.2m	£14.0m	£11.1m	-21%
	Total	**£31.8m**	**£22.8m**	**£26.4m**	**£23.5m**	**-11%**

- 70 per cent (£35.0 million) 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, 80 per cent of all invoice & mandate scam cases reported in 2023 originated via an email
- The reimbursement rate in 2023 was 47 per cent, up slightly from 46 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 purchase scam cases reported and should not be treated as an addition.

	<£1k	>£1k <£10k	>£10k	Total
Cases	599	990	392	1,981
Payments	737	1,329	785	2,851
Value	£0.3m	£3.7m	£16.4m	£20.3m
Returned to victim	£0.2m	£2.5m	£12.7m	£15.4m

- 76 per cent of all losses were returned to the victim in 2023 compared with 61 per cent in 2021

CEO Scam

Value • £11.6m (-14%) **Cases** • 411 (-5%)

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 2020-2023

		2020	2021	2022	2023	CHANGE
Cases	Personal	82	65	50	29	-42%
	Non-Personal	275	396	382	382	0%
	Total	**357**	**461**	**432**	**411**	**-5%**
Payments	Personal	127	99	80	36	-55%
	Non-Personal	360	579	535	555	4%
	Total	**487**	**678**	**615**	**591**	**-4%**
Value	Personal	£0.9m	£1.1m	£0.6m	£0.3m	-42%
	Non-Personal	£3.9m	£11.6m	£12.9m	£11.2m	-13%
	Total	**£4.8m**	**£12.7m**	**£13.4m**	**£11.6m**	**-14%**
Returned to victim	Personal	£0.5m	£0.7m	£0.3m	£0.1m	-85%
	Non-Personal	£1.5m	£2.4m	£3.2m	£3.0m	-6%
	Total	**£2.0m**	**£3.1m**	**£3.6m**	**£3.1m**	**-14%**

- CEO scam is the smallest of all eight scam types in both loss and case volume: accounting for only 2.5 per cent of the total loss and less than 0.2 per cent of the overall case volumes
- 97 per cent of all CEO scam losses occurred on a non-personal account
- The average case value was over £28,000, the highest of all eight scam types
- The reimbursement rate in 2023 was 27 per cent, down from 41 per cent in 2020. Given the low volumes and high values associated with this category, one large case can have a significant impact on reimbursement rates and trends over time.

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 purchase scam cases reported and should not be treated as an addition.

	<£1k	>£1k <£10k	>£10k	Total
Cases	15	116	39	170
Payments	20	133	82	235
Value	£0.01m	£0.6m	£1.1m	£1.7m
Returned to victim	£0.01m	£0.3m	£0.5m	£0.8m

- 48 per cent of all losses were returned to the victim in 2023 compared with 61 per cent in 2021

Impersonation: Police / Bank Staff

Value • £78.9m (-28%) **Cases** • 10,594 (-37%)

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 2020-2023

		2020	2021	2022	2023	CHANGE
Cases	Personal	20,199	28,629	16,413	10,088	-39%
	Non-Personal	978	777	535	506	-5%
	Total	**21,177**	**29,406**	**16,948**	**10,594**	**-37%**
Payments	Personal	37,232	60,931	47,139	29,237	-38%
	Non-Personal	3,365	1,875	1,391	1,515	9%
	Total	**40,597**	**62,806**	**48,530**	**30,752**	**-37%**
Value	Personal	£84.3m	£130.3m	£100.7m	£67.8m	-33%
	Non-Personal	£6.6m	£7.0m	£9.1m	£11.1m	22%
	Total	**£90.9m**	**£137.3m**	**£109.8m**	**£78.9m**	**-28%**
Returned to victim	Personal	£53.9m	£80.7m	£76.0m	£55.3m	-27%
	Non-Personal	£4.2m	£4.1m	£6.3m	£6.1m	-3%
	Total	**£58.0m**	**£84.8m**	**£82.3m**	**£61.4m**	**-25%**

- Lowest loss total ever reported
- Lowest case volume total ever reported
- Nealy all cases (96 per cent) were enabled by telecommunications
- The reduction is likely to be driven by a positive impact from extensive messaging to consumers, for example, advertising campaigns such as Take Five, key messages and warning messages during the payment journey, and industry messaging educating consumers on banks behaviours that they will never request personal information on a bank-initiated call
- The reimbursement rate in 2023 was 78 per cent; the highest of all eight scam types

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 purchase scam cases reported and should not be treated as an addition.

	<£1k	>£1k <£10k	>£10k	Total
Cases	3,251	4,755	1,693	9,699
Payments	5,833	15,574	7,508	28,915
Value	£1.4m	£18.1m	£48.7m	£68.2m
Returned to victim	£1.1m	£14.1m	£38.6m	£53.9m

- 79 per cent of all losses were returned to the victim in 2023 compared with 60 per cent in 2020

Impersonation: Other

Value • £57.3m (-16%) **Cases** • 23,563 (-17%)

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 2020-2023

		2020	2021	2022	2023	CHANGE
Cases	Personal	18,341	25,233	27,463	22,535	-18%
	Non-Personal	1,387	994	956	1,028	8%
	Total	**19,728**	**26,227**	**28,419**	**23,563**	**-17%**
Payments	Personal	30,824	42,643	45,608	36,558	-20%
	Non-Personal	2,510	1,983	1,468	1,621	10%
	Total	**33,334**	**44,626**	**47,076**	**38,179**	**-19%**
Value	Personal	£50.4m	£70.1m	£61.3m	£51.9m	-15%
	Non-Personal	£5.4m	£7.4m	£6.5m	£5.4m	-17%
	Total	**£55.8m**	**£77.5m**	**£67.8m**	**£57.3m**	**-16%**
Returned to victim	Personal	£26.2m	£36.8m	£39.6m	£37.8m	-5%
	Non-Personal	£2.3m	£2.6m	£2.7m	£2.6m	-4%
	Total	**£28.6m**	**£39.4m**	**£42.3m**	**£40.4m**	**-5%**

- Losses were 16 per cent lower and case numbers 17 per cent lower in 2023 compared with 2022.
- 76 per cent of cases were enabled by telecommunications
- The reimbursement rate in 2023 was 71 per cent; the second 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 purchase scam cases reported and should not be treated as an addition.

	<£1k	>£1k <£10k	>£10k	Total
Cases	12,353	8,711	504	21,568
Payments	15,608	16,096	2,894	34,598
Value	£6.51m	£22.4m	£21.5m	£50.4m
Returned to victim	£4.84m	£15.0m	£15.9m	£35.8m

- 71 per cent of all losses were returned to the victim when assessed using the voluntary code in 2023 compared with 45 per cent in 2020

Payment Type

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

		2020	2021	2022	2023	CHANGE
Faster Payment	Payments	236,641	335,451	364,964	409,533	12%
	Value	£349.4m	£504.5m	£421.1m	£380.2m	-10%
CHAPS	Payments	501	764	550	449	-18%
	Value	£14.5m	£22.5m	£13.9m	£23.1m	66%
BACs	Payments	1,193	1,695	2,227	2,530	14%
	Value	£23.5m	£20.4m	£24.0m	£27.9m	16%
Intra bank transfer	Payments	3,113	3,358	1,242	1,645	33%
	Value	£10.6m	£7.5m	£1.5m	£2.6m	70%
International	Payments	3,123	3,869	3,283	3,302	1%
	Value	£22.7m	£28.3m	£24.7m	£25.9m	5%
Total	**Payments**	**244,571**	**345,137**	**372,266**	**417,459**	**12%**
	Value	**£420.7m**	**£583.2m**	**£485.2m**	**£459.7m**	**-5%**

- Faster Payments was used for 98 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 five per cent of the total value

Payment Channel

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

		2020	2021	2022	2023	CHANGE
Branch	Payments	8,968	8,251	8,565	8,175	-5%
	Value	£43.6m	£56.6m	£45.7m	£50.0m	9%
Internet Banking	Payments	113,853	130,016	138,700	123,457	-11%
	Value	£262.5m	£329.1m	£274.6m	£224.9m	-18%
Telephone Banking	Payments	5,593	6,249	6,176	6,618	7%
	Value	£17.8m	£24.4m	£15.6m	£18.9m	21%
Mobile Banking	Payments	116,157	200,621	218,809	279,209	28%
	Value	£96.9m	£173.2m	£149.3m	£165.9m	11%
Total	**Payments**	**244,571**	**345,137**	**372,250**	**417,459**	**12%**
	Value	**£420.7m**	**£583.2m**	**£485.2m**	**£459.7m**	**-5%**

- The most common payment channel was mobile banking which accounted for 67 per cent of the payment volume and 36 per cent of the loss, indicating the typically lower payment limits available to customers within the mobile banking channel.

10

Annex

Gross Losses: All Categories 2020 - 2023

TYPE	CATEGORY	SUB CATEGORY	2020	2021	2022	2023	CHANGE
UNAUTHORISED	CARD	Lost & stolen	£78.9m	£77.2m	£100.2m	£104.0m	4%
UNAUTHORISED	CARD	CNR	£4.4m	£3.9m	£4.0m	£3.0m	-24%
UNAUTHORISED	CARD	Counterfeit	£8.7m	£4.7m	£4.7m	£4.7m	0%
UNAUTHORISED	CARD	Remote purchase	£452.6m	£412.5m	£395.7m	£360.5m	-9%
UNAUTHORISED	CARD	Card ID Theft	£29.7m	£26.3m	£51.7m	£79.1m	53%
UNAUTHORISED	CHEQUE	Cheque	£12.3m	£6.4m	£7.5m	£5.6m	-25%
UNAUTHORISED	REMOTE BANKING	Internet Banking	£159.7m	£158.3m	£114.1m	£88.7m	-22%
UNAUTHORISED	REMOTE BANKING	Telephone Banking	£16.1m	£15.5m	£14.7m	£17.6m	19%
UNAUTHORISED	REMOTE BANKING	Mobile Banking	£21.6m	£25.8m	£34.2m	£45.5m	33%
AUTHORISED	PAYMENT	Invoice & Mandate scam	£68.8m	£56.7m	£49.5m	£50.3m	2%
AUTHORISED	PAYMENT	CEO scam	£4.8m	£12.7m	£13.4m	£11.6m	-14%
AUTHORISED	PAYMENT	Impersonation: Police/Bank	£90.9m	£137.3m	£109.8m	£78.9m	-28%
AUTHORISED	PAYMENT	Impersonation: Other	£55.8m	£77.5m	£67.8m	£57.3m	-16%
AUTHORISED	PAYMENT	Purchase scam	£51.1m	£64.1m	£67.0m	£85.9m	28%
AUTHORISED	PAYMENT	Investment scam	£109.4m	£171.7m	£114.1m	£107.8m	-5%
AUTHORISED	PAYMENT	Romance scam	£17.8m	£30.9m	£31.3m	£36.5m	17%
AUTHORISED	PAYMENT	Advance Fee scam	£22.2m	£32.1m	£32.2m	£31.3m	-3%

Case Volumes: All Categories 2020 - 2023

TYPE	CATEGORY	SUB CATEGORY	2020	2021	2022	2023	CHANGE
UNAUTHORISED	CARD	Lost & stolen	321,994	325,501	401,340	397,549	-1%
UNAUTHORISED	CARD	CNR	8,435	8,941	8,848	5,933	-33%
UNAUTHORISED	CARD	Counterfeit	52,782	24,908	19,594	18,070	-8%
UNAUTHORISED	CARD	Remote purchase	2,417,866	2,425,099	2,221,026	2,132,331	-4%
UNAUTHORISED	CARD	Card ID Theft	34,545	38,753	82,064	142,442	74%
UNAUTHORISED	CHEQUE	Cheque	1,247	815	966	1,197	24%
UNAUTHORISED	REMOTE BANKING	Internet Banking	55,995	72,557	32,036	13,669	-57%
UNAUTHORISED	REMOTE BANKING	Telephone Banking	7,490	4,623	3,076	3,711	21%
UNAUTHORISED	REMOTE BANKING	Mobile Banking	10,155	11,270	12,361	20,032	62%
AUTHORISED	PAYMENT	Invoice & Mandate scam	4,721	4,330	3,340	3,110	-7%
AUTHORISED	PAYMENT	CEO scam	357	461	432	411	-5%
AUTHORISED	PAYMENT	Impersonation: Police/Bank	21,177	29,406	16,948	10,594	-37%
AUTHORISED	PAYMENT	Impersonation: Other	19,728	26,227	28,419	23,563	-17%
AUTHORISED	PAYMENT	Purchase scam	84,292	99,733	117,170	156,516	34%
AUTHORISED	PAYMENT	Investment scam	8,181	12,074	10,085	10,226	1%
AUTHORISED	PAYMENT	Romance scam	2,325	3,270	3,649	4,160	14%
AUTHORISED	PAYMENT	Advance Fee scam	13,833	20,495	27,329	23,849	-13%

Contributing Members

List of members who have contributed data to this publication

Allied Irish Bank
American Express
Arbuthnot Latham & Co. Limited
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
Secure Trust Bank
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.

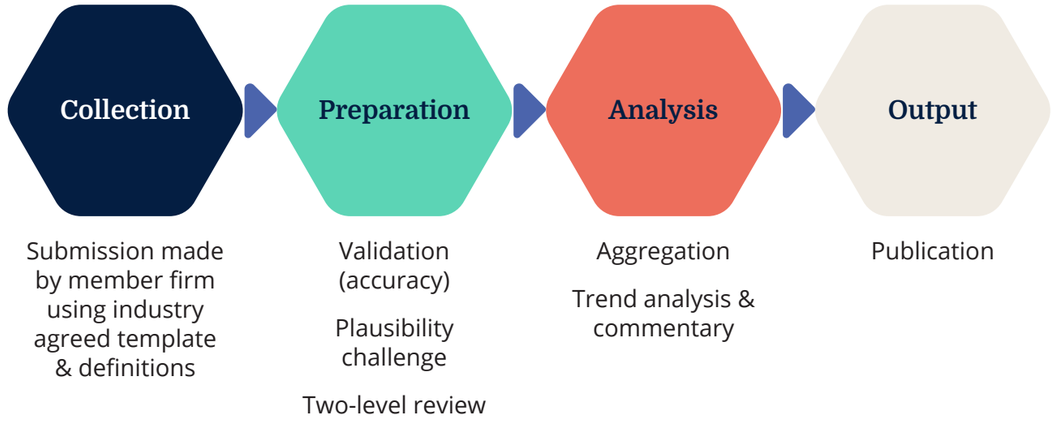
Data plausibility - inputs

Arithmetically correct data for individual members is subject to 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.

ukfinance.org.uk