UK Finance

Half Year Fraud Report

October 2024

In Association with feedzai

Contents

Foreword UK Finance 4

Drivers behind the figures 6

Our fraud data 8

Total Unauthorised Fraud (Cards, Cheques and Remote Banking) 9

Total Authorised Push Payment Fraud 9

Unauthorised Payment Card Fraud 10

Remote Purchase (Card Not Present) 10

Lost And Stolen Card Fraud 11

Card Not Received 11

Card Id Theft 12

Further card fraud analysis 13

UK Retail Face To Face Fraud 13

UK Cash Machine Fraud 13

UK / International Card Fraud 13

Unauthorised Cheque Fraud 14

Remote Banking Fraud 15

Internet Banking 15

Telephone Banking Fraud 16

Mobile Banking Fraud 16

Authorised Push Payment Fraud 17
APP Fraud Enablers 18
The Data: 19
APP Voluntary Code 20
Further Analysis Of The APP Scam Data 20
App Scam Types 21
Purchase Scam 21
Investment Scam 22
Romance Scam 23
Advance Fee Scam 24
Invoice And Mandate Scam 25
CEO Scam 26
Impersonation: Police Or Bank Staff 27
Payment Type 29
Payment Channel 29
Contributing Members 30
Our fraud data 31
Appendix 33

Foreword UK Finance

Fraud continues to pose a major threat to the UK and cause serious harm to individuals and society. In the first half of 2024 just over £570 million was stolen in payment fraud as criminals continue to ruthlessly target people and try to deceive them into making payments or providing enough information to enable their accounts to be accessed or controlled.

As well as the financial losses, this crime can cause severe psychological harm to victims. The best way to protect against fraud is to prevent it from happening in the first place. This is the focus of the financial services industry which invests huge sums of money, including deploying a wide variety of sophisticated tools, to try and detect potential fraud and intervene before it happens. In the first half of this year over £710 million of unauthorised fraud was prevented, an increase of 13 per cent.

Our data once again demonstrates that most fraud originates on social media sites and via telecommunications networks. It is here that most of the social engineering and harm takes place. There have been some notable improvements made by these sectors, but their actions do not yet fully match the scale of the problem.

We need the social media, technology, and telecommunications sectors to do far more in partnership with us to protect the public and society from fraud. Intelligence must flow in both directions and be shared with law enforcement. There should be effective user verification and online marketplaces should use proper payment systems. And there needs to be a commercial incentive for them to act – these sectors should contribute to the cost of countering fraud and victim reimbursement.

For those that do fall victim to authorised push payment (APP) fraud, new reimbursement rules came into force on 7 October 2024. These build on a voluntary code that has been in place for several years and will result in an increased proportion of APP fraud losses being reimbursed and a more consistent approach across the industry. These new rules operate alongside the existing approach to unauthorised fraud whereby almost all losses are reimbursed.

We have always been clear that reimbursement is important in the fight against fraud but can only ever be part of the solution. On its own it does nothing to prevent or reduce the psychological harms to victims, nor does it prevent organised crime groups from stealing money.

We know that criminals try and get people to act quickly, making them believe that if they do not their money is at risk. The government has recently announced changes to give banks and other payment firms the ability to delay and investigate payments that are suspected of being fraudulent. This is an important change and something we have long called for as part of efforts to protect consumers. It could allow firms time to contact customers and give them the advice and support they need to avoid being tricked by criminals. It will however, only be used in relation to a very small number of payments – it is not about stopping or delaying

legitimate payments; rather, it is another tool we can use in the fight to stop this crime.

Our Take Five to Stop Fraud campaign continues to give clear advice to the public on how they can take steps to protect themselves from these crimes. It is easy to think that you will not be a victim of fraud, but it is now such a prevalent crime in this country, and a sophisticated one, that everyone needs to be on guard. Taking a moment to stop and think before parting with your money or information could keep you safe.

We also operate a range of partnerships with government departments, regulators, and law enforcement, including funding a specialist police unit, the Dedicated Card and Payment Crime (DCPCU). These are key parts of the fight against fraud and bringing perpetrators to justice. In 2023 the work of the DCPCU saw 149 subjects arrested or interviewed under caution, 68 offenders convicted and almost 25,000 compromised UK card numbers recovered from criminal gangs.

Sadly, there is no one silver bullet and we know criminals will keep adapting. To stand the best chance of tackling fraud we all need to keep working to reduce the threat it poses.

Ben Donaldson
Managing Director, Economic Crime

Drivers behind the figures

UK Finance's mid-year fraud update for 2024 shows that the total number of cases rose by 16 per cent in the first half of this year compared with the same period last year, but with a 1.5 per cent fall in the value of losses across both authorised and unauthorised fraud. This provides a continuing reminder of the ongoing threat from fraudsters and the harm they pose to consumers.

In the first six months of 2024 our data show diverging trends in unauthorised and authorised payment fraud. The main contributor to the overall increase in fraud cases is unauthorised fraud, primarily through cards, which saw a 19 per cent increase in cases and a seven per cent increase in losses compared with the same period last year. This takes H1 losses for unauthorised card fraud to the highest level since 2020, and 2024 H1 cases were the highest since the first six months of 2018.

There was a particularly large rise in remote purchase fraud, following steady decreases in the previous two years. Cases were up more than a quarter year-on-year, taking them back to levels seen in H1 2021. We had previously attributed declines in recent years to the introduction of Strong Customer Authentication across the industry between 2019 and 2022. In our 2024 Annual Fraud Report we noted that these new rules had helped reduce but had not eliminated this fraud type as criminals still try to circumvent these additional protections by tricking customers into divulging their one-time passcodes (OTPs). Industry feedback points to fraudsters becoming more adept at compromising these security measures.

There were, however, declines in losses and cases across counterfeit and card ID theft. Additionally, continuing investment in advanced detection systems by banks delivered a eight per cent increase in prevented losses in H1, the highest value in our series and representing £6.68 prevented in every £10 of attempted card fraud.

There was also a significant increase (34 per cent) in prevented losses across remote banking. In addition, the value of reported fraud cases and losses continued to fall from the highs of H1 2021. However, within this, declines in cases and losses were concentrated in internet banking with some offsetting increases across telephone and mobile channels. Growth in the latter corresponds with its increasingly widespread use amongst customers.

Turning to authorised push payment (APP) fraud, in which fraudsters trick the victim into making the payment themselves, there was a 16 per cent decline in cases and an 11 per cent fall in losses in the first six months of 2024 compared with the same period in 2023. Notably, our data show falls in cases numbers across all categories of APP fraud in H1. There were decreases in losses across most but not all categories (notable exceptions were CEO, purchase and advance fee).

Our data reports material falls in impersonation fraud cases and losses (both Police/Bank and other) in the first half of the year, suggesting that industry campaigns and cross sector collaboration to block impersonation calls are continuing to bear down on losses from these particular types of scams. As we have seen in some aspects of unauthorised fraud, however, progress cannot be taken for granted as fraudsters continuously evolve their tactics in response to industry's prevention efforts.

Positively, H1 2024 also brought a reduction in romance scams. There was a near doubling of these cases between H1 2020 and H1 2023, leading to a significant increase in not just financial but also psychological harm to the victims. It is likely that scams initiated during the pandemic lockdowns have been identified, and heightened awareness of the risk from this scam type is helping to reduce the flow of new cases.

Ahead of the introduction of mandatory reimbursement of APP fraud (subject to the requirements of the consumer standard of caution), the proportion of losses returned to the victim of APP fraud has decreased in H1 2024 (59.3 per cent) compared with a year ago (63.8 per cent). There were, nevertheless, further rises in the rate of reimbursement to victims of advance fee, romance, and purchase scams.

While the banking and payments industry works to recover and return the losses from this type of fraud, UK Finance data on the enablers of fraud show that little has moved since we started to collect and publish the source of APP fraud. In the first six months of 2024, the main enabler continued to be online platforms, accounting for 72 per cent of cases and 32 per cent of losses. Telecoms-enabled APP fraud continues to be of higher average value – accounting for 16 per cent of cases and 35 per cent of losses.

Reimbursement of victims is, therefore, only part of the solution for APP fraud. Continued effort is still required to stop it at source and stem the flow of money getting into the hands of fraudsters and criminals.

Overall, this mid-year fraud update again highlights industry progress on prevention, particularly in relation to unauthorised fraud, but also some reversion to post-Covid trends. Neither industry nor consumers can be complacent as criminals continue to adapt sophisticated tactics to trick consumers and compromise personal data.

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:

- 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.
- All percentage changes relate to H1 (Jan to June) 2024 vs H1 (Jan to June) 2023 unless otherwise stated.

Total Unauthorised Fraud (Cards, Cheques and Remote Banking)

Unauthorised	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Prevented	£852.5m	£763.2m	£733.0m	£632.1m	£590.6m	£577.5m	£631.3m	£620.7m	£710.9m	**13%**
Cases	1,383,352	1,527,157	1,496,840	1,415,627	1,397,765	1,383,546	1,264,275	1,465,532	1,504,173	**19%**
Gross Loss	£374.0m	£409.8m	£397.3m	£333.0m	£352.4m	£374.5m	£341.2m	£367.6m	£358.0m	**5%**

Losses due to unauthorised transactions on cards, cheques and remote banking increased to £358 million in the first half of this year, up five per cent on the previous year.

The number of recorded cases of unauthorised fraud increased by 19 per cent to just over 1.5 million.

There was a rise of 13 per cent in the value of prevented fraud in H1 2024, with banks stopping £710.9 million of unauthorised fraudulent transactions. This equates to the industry preventing £6.65 in every £10 of attempted fraud.

Research indicates that customers are fully refunded in more than 98 per cent of unauthorised fraud cases.

Total Authorised Push Payment Fraud

Note: APP Data prior to 2020 is not directly comparable and it is therefore excluded from this publication

APP	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Cases	69,093	85,521	101,540	94,456	95,167	112,205	116,316	116,113	97,344	**-16%**
Payments	105,069	139,502	172,622	172,515	166,327	205,939	211,560	205,902	178,230	**-16%**
Gross Loss	£188.1m	£232.6m	£301.5m	£281.8m	£241.9m	£243.3m	£239.3m	£220.4m	£213.7m	**-11%**
Returned to Victim	£75.0m	£99.7m	£125.8m	£131.9m	£135.6m	£150.0m	£152.8m	£134.5m	£126.7m	**-17%**

Losses due to authorised push payment scams were £213.7 million in the first six months of 2024.

This was split between personal (£166.5 million) and non-personal (£47.2 million).

In total there were 97,344 cases of APP fraud reported in January to June 2024 (93,917 Personal and 3,427 non personal) a decrease of 16 per cent on the same period in 2023.

£126.7 million was returned to victims in H1 2024 or 59 per cent of the total loss.

Unauthorised Payment Card Fraud

Card	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Prevented	£486.8m	£496.5m	£481.7m	£484.9m	£492.0m	£482.2m	£519.5m	£502.2m	£558.6m	**8%**
Cases	1,352,646	1,482,976	1,444,996	1,378,206	1,371,469	1,361,403	1,245,224	1,445,974	1,487,289	**19%**
Gross Loss	£287.9m	£286.4m	£261.3m	£263.2m	£270.2m	£286.0m	£260.0m	£291.4m	£277.7m	**7%**

This covers fraud on debit, credit, charge, and ATM-only cards issued in the UK. Payment card fraud losses are organised into five categories:

Remote card purchase | Lost and stolen | Card not received | Counterfeit card | Card ID theft

Fraud losses on cards totalled £277.7 million in the first half of 2024, an increase of seven per cent on the same period in 2023.

Over this period, overall value of card spending by UK card holders grew by 0.3 per cent. Card fraud as a proportion of card purchases has increased from 6.5p in the first half of 2023 to 6.8p in the first half of 2024. A total of £558.6 million of card fraud was stopped by banks and card companies in the first six months of 2024. This is equivalent to £6.68 in every £10 of attempted card fraud prevented without a loss occurring.

Remote Purchase (Card Not Present)

CNP	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Cases	1,134,399	1,283,467	1,264,562	1,159,264	1,136,886	1,084,140	984,059	1,143,142	1,244,157	**26%**
Gross Loss	£222.8m	£229.8m	£210.1m	£202.4m	£198.1m	£197.6m	£174.5m	£186.0m	£193.7m	**11%**

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

Losses due to remote purchase fraud increased by 11 per cent to £193.7 million in the first six months of 2024. The number of cases increased by 26 per cent to just over 1.24 million.

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

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

Contained within these figures, e-commerce card fraud totalled an estimated £145 million in the first half of 2024, a increase of 12 per cent when compared with the same period in 2023.

Lost And Stolen Card Fraud

Lost & Stolen	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Cases	166,710	155,284	144,713	180,788	185,609	215,731	188,409	209,140	180,400	**-4%**
Gross Loss	£41.1m	£37.8m	£35.1m	£42.1m	£46.9m	£53.2m	£48.6m	£55.4m	£50.7m	**4%**

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.

Losses due to lost and stolen card fraud increased four per cent in H1 2024 and totalled £50.7 million. The number of incidents reported decreased four per cent to just over 180,000 cases.

Card Not Received

CNR	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Cases	4,193	4,242	4,126	4,815	5,093	3,755	2,874	3,059	3,244	**13%**
Gross Loss	£2.1m	£2.3m	£2.0m	£2.0m	£1.9m	£2.0m	£1.4m	£1.6m	£1.9m	**39%**

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.

Card not received fraud losses increased by 39 per cent to £1.9 million during January to June 2024, case volumes increased by 13% in the same period.

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

Counterfeit Card Fraud

Counterfeit	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Cases	28,389	24,393	14,640	10,268	9,664	9,930	8,633	9,437	7,488	**-13%**
Gross Loss	£5.4m	£3.3m	£2.6m	£2.1m	£2.2m	£2.5m	£2.3m	£2.4m	£2.1m	**-10%**

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

Counterfeit card losses totalled £2.1 million in H1 2024, a fall of ten per cent on the total reported in 2023. Case volumes fell by 13 per cent to 7,488, the lowest total on record since data collection began.

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

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

Card Id Theft

Card Id Theft	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Cases	18,955	15,590	16,955	23,071	34,217	47,847	61,249	81,196	52,000	**-15%**
Gross Loss	£16.5m	£13.2m	£11.5m	£14.7m	£21.1m	£30.6m	£33.1m	£46.0m	£29.3m	**-12%**

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 occurs in two ways, through third-party applications or account takeover.

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.

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

Losses from card ID theft fell 12 per cent in the first six months of 2024 compared with the same period in 2023, from £33.1 million to £29.3 million. The number of individual cases also decreased over the same period, dropping by 15% to 52,000 cases.

Both types of fraud associated with Card ID theft require the compromise of significant amounts of customers' personal information which is then used to impersonate victims. It is believed this type of fraud is a result of fraudsters focused efforts to target victims' personal information using methods including phishing emails, scam texts and the theft of mail from external mailboxes and multi-occupancy buildings which is then used to target the customers' existing accounts or apply for credit cards by impersonating the victim.

Further card fraud analysis

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

UK Retail Face To Face Fraud

UK Face To Face	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Gross Loss	£25.5m	£23.3m	£19.6m	£27.3m	£33.3m	£38.8m	£38.4m	£50.3m	£36.6m	**-4%**

UK retail face-to-face fraud covers all transactions that occur in person in a UK shop and includes contactless fraud.

Most of this fraud occurs using cards obtained through low-tech methods such as distraction thefts and entrapment devices at ATMs, combined with shoulder surfing or PIN pad cameras to obtain both the card and PIN. Criminals also use methods to dupe victims into handing over their cards on their own doorstep.

This figure includes contactless fraud, contactless fraud covers fraud on both contactless cards and mobile devices.

The industry continues to deploy a range of fraud prevention and detection tools to protect consumers from contactless card fraud and these tools remain highly effective in the fight against this type of fraud. Each card has an inbuilt security feature which means that from time to time, cardholders making a contactless transaction will be asked to enter their PIN to prove they are in possession of their card. The frequency of this varies between card issuers.

UK Cash Machine Fraud

UK ATM	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Gross Loss	£15.0m	£13.1m	£12.0m	£12.4m	£12.9m	£13.2m	£12.7m	£12.9m	£12.8m	**1%**

These figures cover fraud transactions made at cash machines in the UK using a compromised card. In all cases the fraudster would require both the genuine PIN and card.

Losses at UK cash machines increased by one per cent in the first half of 2024, compared with the same period in 2023.

Most of this fraud is thought to be perpetuated through distraction thefts and card entrapment at ATMs.

UK / International Card Fraud

UK/INT	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
UK Gross Loss	£208.5m	£206.0m	£187.6m	£196.4m	£202.4m	£213.8m	£197.2m	£219.7m	£201.6m	**2%**
Int Gross Loss	£79.4m	£80.4m	£73.7m	£66.8m	£67.9m	£72.2m	£62.8m	£71.7m	£76.0m	**21%**

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

Both categories increased in the first half of 2024, UK card fraud losses by two per cent to £201.6 million and international fraud losses by 21 per cent, to £76 million.

Unauthorised Cheque Fraud

Cheque	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Prevented	£184.2m	£54.3m	£21.0m	£12.0m	£10.5m	£9.3m	£7.3m	£5.0m	£11.9m	**63%**
Cases	709	538	382	433	415	551	559	638	647	**16%**
Gross Loss	£6.4m	£5.8m	£3.5m	£2.9m	£3.2m	£4.3m	£2.9m	£2.8m	£3.8m	**32%**

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

- Counterfeit cheques are printed on non-bank paper to look exactly like genuine cheques and are drawn by a fraudster on genuine accounts.
- Forged cheques are genuine cheques that have been stolen from an innocent customer and used by a fraudster with a forged signature.
- Fraudulently altered cheques are genuine cheques that have been made out by the genuine customer but have been altered in some way by a criminal before being paid in, e.g. by changing the beneficiary's name or the amount of the cheque

Losses from cheque fraud increased by 32 per cent in the first half of 2024, while the number of cases rose 16 per cent to 647 cases.

It should be noted that the volume and value of cheque fraud remains very low, and while increases have been reported in 2024, they are not considered to be significant.

Remote Banking Fraud

Remote Banking	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Prevented	£181.5m	£212.3m	£230.3m	£135.3m	£88.1m	£86.0m	£104.6m	£113.5m	£140.4m	**34%**
Cases	29,997	43,643	51,462	36,988	25,881	21,592	18,492	18,920	16,237	**-12%**
Gross Loss	£79.7m	£117.6m	£132.5m	£67.0m	£78.9m	£84.2m	£78.3m	£73.4m	£76.5m	**-2%**

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.

Total remote banking fraud amounted to £76.5 million in the first half of 2024, a two per cent decrease compared to the amount lost in the first six months 2023. The number of cases of remote banking fraud decreased, falling by 12 per cent to 16,237.

UK Finance research shows that last year, 87 per cent of the adult population used at least one form of remote banking.

A total of £140.4 million of attempted remote banking fraud was stopped by bank security systems in the first six months of 2024. This is equivalent to 65p in every £1 of fraud attempted being prevented.

In addition, 19 per cent (£14.2 million) of the losses across all remote banking channels were recovered after the incident.

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

Internet Banking

INT Banking	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Cases	21,312	34,683	42,628	29,929	18,001	14,035	7,775	5,894	4,922	**-37%**
Gross Loss	£64.3m	£95.4m	£108.0m	£50.3m	£55.5m	£58.6m	£50.5m	£38.2m	£45.2m	**-11%**

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.

Typically, criminals employ a range of social engineering techniques to trick victims into giving away their personal and financial information, such as their internet banking one-time passcodes and log in details. This includes using impersonation scam calls, emails or text messages typically exploiting current affairs by impersonating trusted organisations such as HMRC, internet service providers (ISPs) and e-commerce companies. The stolen details are then used to access a customer's online account and to make an unauthorised transaction.

Criminals also abuse remote access software applications to gain control of their victim's online banking facilities. The criminals will typically claim to be providing support from an IT service or internet service provider and convince the customer to download and install remote access applications to their laptop or PC.

Internet banking fraud losses decreased during H1 2024, falling 11 per cent to £45.2 million when compared with the same period in 2023. Case volumes also reduced, falling by 37 per cent to 4,922.

Telephone Banking Fraud

TEL Banking	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Cases	4,681	2,809	2,545	2,078	1,776	1,300	1,533	2,178	1,725	**13%**
Gross Loss	£7.9m	£8.1m	£7.5m	£8.0m	£7.4m	£7.3m	£7.3m	£10.3m	£8.7m	**20%**

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

Like internet banking fraud, criminals often use social engineering tactics to trick customers into revealing their account security details, which are then used to convince the telephone banking operator that they are the genuine account holder.

Losses from telephone banking fraud increased by 20 per cent to £8.7 million in the first six months of 2024. The number of cases increased by 13 per cent to 1,725.

Mobile Banking Fraud

MOB Banking	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Cases	4,004	6,151	6,289	4,981	6,104	6,257	9,184	10,848	9,590	**4%**
Gross Loss	£7.5m	£14.0m	£17.1m	£8.7m	£16.0m	£18.2m	£20.6m	£24.9m	£22.6m	**10%**

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

Rises are to be expected in the mobile banking channel as the level of usage increases amongst customers. Last year, around 60 per cent of adults living in the UK used a mobile banking app either on their telephone or tablet, up from 33 per cent in 2015.

Losses from mobile banking fraud increased by 10 per cent to £22.6 million in the first six months of 2024, the highest recorded total for the first six months of a year since we began collecting data for this fraud type in 2015. The number of cases increased by 4 per cent to 9,590; another record high for the first half of the year.

Authorised Push Payment Fraud

In an authorised push payment scam, a criminal will trick their victim into sending money directly from their account to an account which the criminal controls.

Criminals' use of social engineering tactics through deception and impersonation scams is a key driver of authorised push payment scams and, as highlighted earlier in the report, the use of social engineering tactics to defraud people remains a key driver behind the losses. Typically, such deception and impersonation scams involve the criminal posing as a genuine individual or organisation and contacting the victim using a range of methods including via the telephone, email, and text message. Criminals also use social media to approach victims, using adverts for goods and investments which never materialise once the payment has been made.

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.

		H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Personal	Cases	66,291	78,916	98,102	90,862	92,186	108,457	112,451	112,243	93,917	**-16%**
	Payments	100,977	127,969	167,003	166,748	161,680	200,081	205,472	199,626	172,635	**-16%**
	Loss	£151.9m	£195.5m	£261.8m	£244.1m	£203.0m	£205.2m	£196.7m	£179.7m	£166.5m	**-15%**
	Return To Customer	£63.5m	£85.4m	£112.6m	£120.8m	£120.2m	£133.9m	£136.3m	£120.1m	£108.6m	**-20%**
Non-Personal	Cases	2,802	6,605	3,438	3,594	2,981	3,748	3,865	3,870	3,427	**-11%**
	Payments	4,092	11,533	5,619	5,767	4,647	5,858	6,088	6,276	5,595	**-8%**
	Loss	£36.2m	£37.1m	£39.6m	£37.7m	£38.9m	£38.1m	£42.6m	£40.6m	£47.2m	**11%**
	Return To Customer	£11.5m	£14.3m	£13.2m	£11.1m	£15.4m	£16.1m	£16.5m	£14.3m	£18.1m	**10%**
Overall	Cases	69,093	85,521	101,540	94,456	95,167	112,205	116,316	116,113	97,344	**-16%**
	Payments	105,069	139,502	172,622	172,515	166,327	205,939	211,560	205,902	178,230	**-16%**
	Loss	£188.1m	£232.6m	£301.4m	£281.8m	£241.9m	£243.3m	£239.3m	£220.4m	£213.7m	**-11%**
	Return To Customer	£75.0m	£99.7m	£125.8m	£131.9m	£135.6m	£150.0m	£152.8m	£134.5m	£126.7m	**-17%**

Losses due to authorised push payment scams were £213.7 million in the first six months of 2024, a decrease of 11 per cent when compared with the same period in 2023. This was split between personal (£166.5 million) and non-personal (£47.2 million). In total there were 97,344 cases of APP fraud reported in January to June 2024 (93,917 Personal and 3,427 non personal) a decrease of 16 per cent on the same period in 2023.

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

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

This shows that:

- 72% of fraud cases are enabled by online sources. These cases tend to include lower-value scams such as purchase fraud and therefore account for 32% of total losses.
- 16% of fraud cases are enabled by telecommunications, these are usually higher value cases such as impersonation scams and so account for 35% of losses .

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

	Volume	Value
Online	72%	32%
Telecommunications	16%	35%
Email	1%	10%
Other	3%	6%
Unable to ascertain	8%	17%

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.

APP Voluntary Code

In 2019, following work between the industry, consumer groups and the regulator, an authorised push payment (APP) scams voluntary code was introduced. The code was designed to deliver protections for customers of signatory payment service providers (PSPs) and delivers a commitment from all firms who sign up to it to reimburse victims of authorised push payment scams in any scenario where their bank or payment service provider is at fault and the customer has met the standards expected of them under the code.

UK Finance collates and publishes statistics relating to the cases assessed using the voluntary code. Data show that 89,685 cases have been assessed and closed during H1 2024, with a total value of £150 million. Of this, £98.3 million was reimbursed to victims (66 per cent of the total). Of the 89,685 reported, 82 per cent involved values of less than £1,000, whilst only three per cent of cases involved sums of more than £10,000.

		H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	CHANGE
Less than £1k	Cases	49,992	54,347	66,820	60,591	64,086	77,860	86,937	87,825	73,648	-15%
	Payments	62,220	68,438	84,320	81,205	87,357	108,826	123,466	121,679	102,006	-17%
	Loss	£13.1m	£16.5m	£20.3m	£17.6m	£16.3m	£19.6m	£20.0m	£20.5m	£17.5m	-12%
	Returned to Victim	£4.4m	£5.5m	£7.4m	£7.8m	£10.1m	£13.6m	£15.2m	£15.6m	£13.8m	-9%
£1k-£10k	Cases	12,583	18,326	24,793	22,343	20,661	21,775	17,314	16,680	13,598	-21%
	Payments	25,970	39,428	57,457	50,966	46,844	54,359	48,126	45,182	39,711	-17%
	Loss	£41.2m	£60.6m	£80.3m	£68.7m	£62.9m	£63.9m	£52.8m	£49.6m	£40.7m	-23%
	Returned to Victim	£17.8m	£27.6m	£36.6m	£33.6m	£37.9m	£39.8m	£33.6m	£31.9m	£27.2m	-19%
Over 10k	Cases	2,657	3,355	4,497	4,001	3,149	3,322	3,162	2,606	2,439	-23%
	Payments	8,760	13,181	18,693	21,966	19,562	24,590	23,597	23,110	23,135	-2%
	Loss	£84.8m	£99.8m	£142.1m	£140.4m	£117.3m	£108.0m	£114.6m	£93.5m	£91.8m	-20%
	Returned to Victim	£40.0m	£49.1m	£70.9m	£70.3m	£69.2m	£68.5m	£79.9m	£64.3m	£57.3m	-28%
Overall	Cases	65,232	76,028	96,110	86,935	87,896	102,957	107,413	107,111	89,685	-17%
	Payments	96,950	121,047	160,470	154,137	153,763	187,775	195,189	189,971	164,852	-16%
	Loss	£139.1m	£176.9m	£242.7m	£226.7m	£196.6m	£191.6m	£187.4m	£163.6m	£150.0m	-20%
	Returned to Victim	£62.2m	£82.3m	£114.9m	£111.7m	£117.2m	£121.9m	£128.7m	£111.9m	£98.3m	-24%

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.

App Scam Types

Purchase Scam

Purchase Scam	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Cases	40,486	43,806	50,327	49,406	53,907	63,263	76,943	79,573	68,409	**-11%**
Payments	50,933	56,560	64,948	67,463	72,282	86,836	107,655	111,939	97,326	**-10%**
Loss	£23.9m	£27.2m	£32.3m	£31.8m	£31.1m	£35.9m	£40.9m	£45.1m	£42.3m	**3%**
Returned to Victim	£6.5m	£8.1m	£9.3m	£11.7m	£16.5m	£21.6m	£25.7m	£30.1m	£27.9m	**9%**

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 scams continued to be the most common form of APP scam with 68,409 confirmed cases accounting for 70 per cent of the total number of all APP scam cases reported in the first half of 2024. A total of £42.3 million was lost to purchase scams during the same period; Losses are now at their highest point since we began collecting data in 2020.

Payment service providers returned £27.9 million (66%) of the losses to the victims.

Voluntary Code: Purchase scam 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 therefore should not be treated as an addition.

CODE ONLY: Purchase Scam	Less than £1k	£1k-£10k	More than £10k	Total
Cases	58,037	5,914	326	**64,277**
Payments	76,577	12,971	2,004	**91,552**
Value	£11.7m	£16.8m	£8.3m	**£36.8m**
Returned to customer	£9.2m	£10.6m	£4.6m	**£24.5m**

For those cases which were applicable for assessment using the voluntary code during the first half of 2024, 67 per cent of all losses were returned to the victim compared with 63 per cent in the same period for 2023. 90 per cent of all cases assessed involved case values of less than £1,000.

Investment Scam

Investment Scam	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Cases	3,655	4,526	6,224	5,850	5,161	4,924	5,112	5,114	3,647	**-29%**
Payments	8,720	11,203	17,567	18,098	14,928	15,583	16,942	16,454	12,959	**-24%**
Loss	£47.6m	£61.8m	£90.6m	£81.1m	£58.4m	£55.7m	£57.2m	£50.7m	£56.4m	**-1%**
Returned to Victim	£14.2m	£22.6m	£34.8m	£37.0m	£29.4m	£29.2m	£33.5m	£25.5m	£30.1m	**-10%**

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 losses decreased by one per cent in January to June 2024 to £56.4 million. After the peak seen in 2021 during the pandemic losses and case volumes have levelled out, this is likely a combination of factors including fewer opportunities for fraudsters to contact victims now that lockdown restrictions have eased, and also the emergence of cost-of-living pressures meaning individuals are more cautious with money and less likely to be looking for investment opportunities. Investment scams continued to account for the largest value of all eight APP scam types accounting for 26 per cent of the overall total.

The nature of the scams combined with the sophistication of the criminals mean that typically the sums involved in this type of scam are higher so while investment scams account for the largest proportion of loss, they only account for four per cent of the total number of APP scam cases.

Payment service providers returned £30.1 million (53 per cent) of the losses to the victims down from 59 per cent in the first half of 2023.

Voluntary Code: Investment scam 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 therefore should not be treated as an addition.

CODE ONLY: Investment Scam	Less than £1k	£1k-£10k	More than £10k	Total
Cases	1,386	962	691	**3,039**
Payments	2,326	3,667	5,072	**11,065**
Value	£0.5m	£3.8m	£37.8m	**£42.1m**
Returned to customer	£0.3m	£2.1m	£21.0m	**£23.5m**

For those cases which were applicable for assessment using the voluntary code during the first half of 2024, 56 per cent of all losses were returned to the victim compared with 61 per cent in the same period in 2023.

Romance Scam

All Romance Scam	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Cases	1,107	1,218	1,479	1,791	1,644	2,005	2,120	2,040	1,963	**-7%**
Payments	6,051	7,134	11,489	14,325	13,199	17,021	18,889	20,689	21,110	**12%**
Loss	£8.5m	£9.3m	£12.7m	£18.2m	£14.6m	£16.7m	£18.5m	£18.1m	£14.5m	**-21%**
Returned To Victim	£2.9m	£3.1m	£4.3m	£7.8m	£7.2m	£9.3m	£11.6m	£11.2m	£9.4m	**-19%**

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.

A total of £14.5 million was lost to romance scams during January to June 2024, a decrease of 21 per cent when compared with the same period in 2023. Romance scams have an average of nearly eleven 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.

Payment services providers were subsequently able to return £9.4 million to victims or 65 per cent of the total, an increase from the 63 per cent being reimbursed during the same period in 2023.

Voluntary Code: Romance scam 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 therefore should not be treated as an addition.

CODE ONLY: Romance Scam	Less than £1k	£1k-£10k	More than £10k	Total
Cases	953	602	229	**1,784**
Payments	3,491	7,811	8,896	**20,198**
Value	£0.3m	£2.0m	£9.1m	**£11.4m**
Returned to customer	£0.2m	£1.4m	£5.7m	**£7.4m**

For those cases which were applicable for assessment using the voluntary code during the first half of 2024, 65 per cent of all losses were returned to the victim compared with 67 per cent in the same period in 2023.

Advance Fee Scam

Advance Fee Scam	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Cases	5,697	8,136	9,064	11,431	11,472	15,857	12,238	11,611	8,599	**-30%**
Payments	9,245	13,987	16,233	20,737	20,609	30,622	27,047	23,913	18,806	**-30%**
Loss	£8.3m	£13.9m	£14.1m	£18.1m	£14.2m	£18.0m	£15.1m	£16.3m	£15.8m	**5%**
Returned To Victim	£3.0m	£4.5m	£5.3m	£6.1m	£6.3m	£11.5m	£9.6m	£11.7m	£10.5m	**10%**

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 scams were the third most common form of APP scam in the first half of 2024, accounting for nine per cent of the total number of cases. A total of £15.8 million was lost to advance fee scams, an increase of five percent compared with the first six months of 2023.

Payment service providers returned £10.5million (67 per cent) of the losses to the victims up from 64 per cent in the first half of 2023.

Voluntary Code: Advance fee scam 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 therefore should not be treated as an addition.

CODE ONLY: Advance Fee Scam	Less than £1k	£1k-£10k	More than £10k	Total
Cases	6,381	1,140	219	**7,740**
Payments	10,190	3,959	2,907	**17,056**
Value	£1.6m	£3.4m	£7.8m	**£12.8m**
Returned to customer	£1.3m	£2.1m	£4.9m	**£8.3m**

For those cases which were applicable for assessment using the voluntary code during the first half of 2024, 65 per cent of all losses were returned to the victim compared with 64 per cent in the same period for 2023.

Invoice And Mandate Scam

Invoice & Mandate Scam	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Cases	2,778	1,943	2,053	2,277	1,591	1,749	1,665	1,445	1,137	**-32%**
Payments	3,613	2,707	2,813	3,354	2,340	2,625	2,352	2,060	1,598	**-32%**
Loss	£40.1m	£28.6m	£27.1m	£29.6m	£25.5m	£24.0m	£24.8m	£25.4m	£25.7m	**4%**
Returned To Victim	£16.5m	£13.3m	£10.8m	£11.7m	£13.6m	£12.8m	£12.2m	£11.4m	£11.8m	**-3%**

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 and mandate scam losses totalled £25.7 million in the first half of 2024, an increase of four per cent when compared with the same period in 2023.

78 per cent (£20 million) of invoice and mandate scam losses occurred on a non-personal or business account. Typically, businesses make genuine higher-value payments more regularly, making it harder to spot and stop a fraudulent one.

Payment service providers returned £11.8 million (46 per cent) of the losses to the victims down from 49 per cent in the first half of 2023.

Voluntary Code: Invoice and mandate scam 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 therefore should not be treated as an addition

CODE ONLY: Invoice & Mandate Scam	Less than £1k	£1k-£10k	More than £10k	Total
Cases	214	310	109	**633**
Payments	255	427	235	**917**
Value	£0.1m	£1.1m	£4.0m	**£5.3m**
Returned to customer	£0.1m	£0.8m	£3.2m	**£4.1m**

For those cases which were applicable for assessment using the voluntary code during the first half of 2024, 77 per cent of all losses were returned to the victim compared with 74 per cent in the same period for 2023.

CEO Scam

CEO Scam	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	CHANGE
Cases	187	170	230	231	200	232	196	215	158	**-19%**
Payments	235	252	331	347	297	318	302	289	296	**-2%**
Loss	£2.4m	£2.4m	£6.1m	£6.6m	£7.9m	£5.6m	£6.9m	£4.7m	£7.8m	**13%**
Returned to Victim	£1.1m	£0.7m	£1.6m	£1.2m	£2.2m	£1.4m	£1.4m	£1.7m	£1.3m	**-3%**

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 fraud remained the least common form of APP scam in H1 2024, accounting for less than one per cent of total cases. A total of £7.8 million was lost, equivalent to only four per cent of total APP losses. CEO has the highest average case value of all eight scam types with an average of just under £50,000 being lost per confirmed case.

Payment service providers returned £1.3 million (17 per cent) of the losses to the victims down from 20 per cent in the first half of 2023.

Voluntary Code: CEO scam 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 therefore should not be treated as an addition.

CODE ONLY: CEO Scam	Less than £1k	£1k-£10k	More than £10k	Total
Cases	9	40	13	**62**
Payments	9	102	25	**136**
Value	£0.006m	£0.2m	£0.4m	**£0.6m**
Returned to customer	£0.002m	£0.1m	£0.2m	**£0.3m**

For those cases which were applicable for assessment using the voluntary code during the first half of 2024, 57 per cent of all losses were returned to the victim compared with 55 per cent in the same period for 2023.

Impersonation: Police Or Bank Staff

IMP: POL/ BANK STAFF	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Cases	7,983	13,194	17,521	11,885	9,138	7,810	5,976	4,618	4,089	**-32%**
Payments	14,049	26,548	34,774	28,032	22,533	25,997	17,910	12,842	11,015	**-38%**
Loss	£34.7m	£56.1m	£75.6m	£61.8m	£59.4m	£50.4m	£43.5m	£35.4m	£32.3m	**-26%**
Returned to Victim	£20.0m	£32.1m	£40.6m	£38.6m	£42.0m	£40.4m	£35.0m	£26.4m	£22.1m	**-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 in order to make their approach sound genuine.

Police and bank staff impersonation scams accounted for 15 per cent of all APP scam losses in H1 2024 totalling £32.3 million. However, losses have decreased by 26 per cent when compared with the same period in 2023 and case volumes have fallen by 32 per cent in the same period. This is likely to be a result of the investment made by the industry to educate consumers. Prevention methods such as effective warning messages during the payment journey will also have helped contribute to the significant reduction in this type of fraud.

Payment service providers were able to return £22.1 million of the losses to customers or 68 per cent of the total, down from 80 per cent being reimbursed in H1 2023.

Voluntary Code: Impersonation: Police or Bank staff 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 therefore should not be treated as an addition.

CODE ONLY: IMP: Pol / Bank Staff Scam	Less than £1k	£1k-£10k	More than £10k	Total
Cases	1,394	1,670	681	**3,745**
Payments	2,502	5,175	2,767	**10,444**
Value	£0.6m	£6.2m	£19.5m	**£26.3m**
Returned to customer	£0.5m	£4.9m	£14.3m	**£19.7m**

For those cases which were applicable for assessment using the voluntary code during the first half of 2024, 75 per cent of all losses were returned to the victim compared with 79 per cent in the same period for 2023.

Impersonation: Other

IMP: Other Scam	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Cases	7,200	12,528	14,642	11,585	12,054	16,365	12,066	11,497	9,342	**-23%**
Payments	12,223	21,111	24,467	20,159	20,139	26,937	20,463	17,716	15,120	**-26%**
Loss	£22.5m	£33.3m	£43.0m	£34.6m	£30.8m	£37.0m	£32.6m	£24.7m	£18.8m	**-42%**
Returned to Victim	£10.8m	£15.3m	£19.2m	£17.7m	£18.5m	£23.8m	£23.9m	£16.5m	£13.5m	**-44%**

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.

A total of £18.8 million was lost to this type of scam during the first six months of 2024, a decrease of 42 per cent when compared with 2023.

Payment service providers were able to return £13.5million of the losses to customers or 72 per cent of the total.

Voluntary Code: Impersonation: Other 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 therefore should not be treated as an addition.

CODE ONLY: IMP: Other Scam	Less than £1k	£1k-£10k	More than £10k	Total
Cases	5,274	2,960	171	**8,405**
Payments	6,656	5,599	1,229	**13,484**
Value	£2.7m	£7.2m	£4.9m	**£14.8m**
Returned to customer	£2.1m	£5.1m	£3.3m	**£10.5m**

For those cases which were applicable for assessment using the voluntary code during the first half of 2024, 71 per cent of all losses were returned to the victim compared with 76 per cent in the same period for 2023.

Payment Type

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

Payment Type Volumes	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Faster Payment	101,297	135,344	167,720	167,731	163,142	201,822	207,959	201,574	173,061	**-17%**
CHAPS	244	257	435	329	398	152	196	253	144	**-27%**
BACS	667	526	729	966	911	1,316	1,284	1,246	1,073	**-16%**
Intra Bank Transfer (''on us'')	1,402	1,711	2,100	1,258	532	710	812	834	1,675	**106%**
International	1,459	1,664	1,638	2,231	1,344	1,939	1,309	1,993	2,277	**74%**
Total	105,069	139,502	172,622	172,515	166,327	205,939	211,560	205,900	178,230	**-16%**

Payment Type Values	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Faster Payment	£149.3m	£200.1m	£263.7m	£240.8m	£208.3m	£212.8m	£199.1m	£181.1m	£159.8m	**-20%**
CHAPS	£8.2m	£6.3m	£9.3m	£13.2m	£8.8m	£5.1m	£13.1m	£10.0m	£11.6m	**-12%**
BACS	£15.1m	£8.4m	£11.1m	£9.3m	£12.5m	£11.4m	£13.2m	£14.6m	£20.2m	**53%**
Intra Bank Transfer (''on us'')	£2.7m	£7.9m	£5.3m	£2.3m	£0.5m	£1.1m	£1.6m	£1.0m	£3.1m	**92%**
International	£12.9m	£9.9m	£12.2m	£16.2m	£11.8m	£12.9m	£12.3m	£13.6m	£19.0m	**55%**
Total	£188.1m	£232.6m	£301.5m	£281.8m	£241.9m	£243.3m	£239.3m	£220.4m	£213.7m	**-11%**

Payment Channel

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

Payment Channel Volumes	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Branch	3,445	5,523	4,070	4,181	3,754	4,811	4,480	3,695	3,275	**-27%**
Internet Banking	55,608	58,245	62,789	67,227	63,229	75,471	72,370	51,087	41,229	**-43%**
Telephone Banking	2,687	2,906	2,725	3,524	3,203	2,973	3,710	2,908	1,549	**-58%**
Mobile Banking	43,329	72,828	103,038	97,583	96,141	122,668	131,000	148,209	132,177	**1%**
Total	105,069	139,502	172,622	172,515	166,327	205,923	211,560	205,899	178,230	**-16%**

Payment Channel Values	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
Branch	£19.7m	£23.9m	£27.2m	£29.3m	£25.0m	£20.7m	£27.5m	£22.5m	£22.9m	**-17%**
Internet Banking	£126.8m	£135.7m	£171.4m	£157.7m	£135.6m	£139.0m	£129.5m	£95.4m	£96.5m	**-26%**
Telephone Banking	£9.7m	£8.1m	£11.3m	£13.1m	£8.7m	£6.9m	£7.7m	£11.2m	£8.7m	**14%**
Mobile Banking	£32.0m	£64.8m	£91.5m	£81.7m	£72.5m	£76.8m	£74.7m	£91.2m	£85.6m	**15%**
Total	£188.1m	£232.6m	£301.5m	£281.8m	£241.9m	£243.3m	£239.3m	£220.4m	£213.7m	**-11%**

Contributing Members

List of members who have contributed data to this publication

Allied Irish Bank
American Express
Arbuthnot Latham & Co
Bank of Ireland
Barclays Bank
C Hoare & Co
Capital One
Citibank
Coventry Building Society
Danske Bank
Hampden & Co
HSBC
Investec
Lloyds Banking Group
Marks & Spencer
Metro Bank
Modulr
Nationwide
Natwest Group
New Day
Sainsburys Bank
Santander
Secure Trust Bank
Silicon Valley Bank
Starling Bank
Tesco Bank
The Co-operative 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.

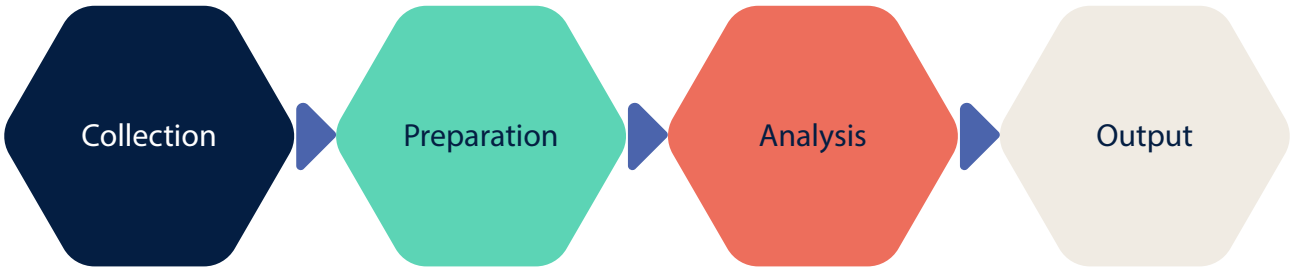
Data plausibility - inputs

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;



Submission made by member firm using industry agreed template & definitions

Validation (accuracy)

Plausibility challenge

Two-level review

Aggregation

Trend analysis & commentary

Publication

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

Appendix

Cases

Type	Category	Sub Category	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
UNAUTHORISED	CARD	Lost & stolen	166,710	155,284	144,713	180,788	185,609	215,731	188,409	209,140	180,400	**-4%**
UNAUTHORISED	CARD	CNR	4,193	4,242	4,126	4,815	5,093	3,755	2,874	3,059	3,244	**13%**
UNAUTHORISED	CARD	Counterfeit	28,389	24,393	14,640	10,268	9,664	9,930	8,633	9,437	7,488	**-13%**
UNAUTHORISED	CARD	Remote purchase	1,134,399	1,283,467	1,264,562	1,159,264	1,136,886	1,084,140	984,059	1,143,142	1,244,157	**26%**
UNAUTHORISED	CARD	Card ID Theft	18,955	15,590	16,955	23,071	34,217	47,847	61,249	81,196	52,000	**-15%**
UNAUTHORISED	CHEQUE	Cheque	709	538	382	433	415	551	559	638	647	**16%**
UNAUTHORISED	REMOTE BANKING	Internet Banking	21,312	34,683	42,628	29,929	18,001	14,035	7,775	5,894	4,922	**-37%**
UNAUTHORISED	REMOTE BANKING	Telephone Banking	4,681	2,809	2,545	2,078	1,776	1,300	1,533	2,178	1,725	**13%**
UNAUTHORISED	REMOTE BANKING	Mobile Banking	4,004	6,151	6,289	4,981	6,104	6,257	9,184	10,848	9,590	**4%**
AUTHORISED	PAYMENT	Invoice & Mandate	2,778	1,943	2,053	2,277	1,591	1,749	1,665	1,445	1,137	**-32%**
AUTHORISED	PAYMENT	CEO	187	170	230	231	200	232	196	215	158	**-19%**
AUTHORISED	PAYMENT	IMP: Police/Bank	7,983	13,194	17,521	11,885	9,138	7,810	5,976	4,618	4,089	**-32%**
AUTHORISED	PAYMENT	IMP: Other	7,200	12,528	14,642	11,585	12,054	16,365	12,066	11,497	9,342	**-23%**
AUTHORISED	PAYMENT	Purchase	40,486	43,806	50,327	49,406	53,907	63,263	76,943	79,573	68,409	**-11%**
AUTHORISED	PAYMENT	Investment	3,655	4,526	6,224	5,850	5,161	4,924	5,112	5,114	3,647	**-29%**
AUTHORISED	PAYMENT	Romance	1,107	1,218	1,479	1,791	1,644	2,005	2,120	2,040	1,963	**-7%**
AUTHORISED	PAYMENT	Advance Fee	5,697	8,136	9,064	11,431	11,472	15,857	12,238	11,611	8,599	**-30%**

Losses

Type	Category	Sub Category	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	Change
UNAUTHORISED	CARD	Lost & stolen	£41.1m	£37.8m	£35.1m	£42.1m	£46.9m	£53.2m	£48.6m	£55.4m	£50.7m	**4%**
UNAUTHORISED	CARD	CNR	£2.1m	£2.3m	£2.0m	£2.0m	£1.9m	£2.0m	£1.4m	£1.6m	£1.9m	**39%**
UNAUTHORISED	CARD	Counterfeit	£5.4m	£3.3m	£2.6m	£2.1m	£2.2m	£2.5m	£2.3m	£2.4m	£2.1m	**-10%**
UNAUTHORISED	CARD	Remote purchase	£222.8m	£229.8m	£210.1m	£202.4m	£198.1m	£197.6m	£174.5m	£186.0m	£193.7m	**11%**
UNAUTHORISED	CARD	Card ID Theft	£16.5m	£13.2m	£11.5m	£14.7m	£21.1m	£30.6m	£33.1m	£46.0m	£29.3m	**-12%**
UNAUTHORISED	CHEQUE	Cheque	£6.4m	£5.8m	£3.5m	£2.9m	£3.2m	£4.3m	£2.9m	£2.8m	£3.8m	**32%**
UNAUTHORISED	REMOTE BANKING	Internet Banking	£64.3m	£95.4m	£108.0m	£50.3m	£55.5m	£58.6m	£50.5m	£38.2m	£45.2m	**-11%**
UNAUTHORISED	REMOTE BANKING	Telephone Banking	£7.9m	£8.1m	£7.5m	£8.0m	£7.4m	£7.3m	£7.3m	£10.3m	£8.7m	**20%**
UNAUTHORISED	REMOTE BANKING	Mobile Banking	£7.5m	£14.0m	£17.1m	£8.7m	£16.0m	£18.2m	£20.6m	£24.9m	£22.6m	**10%**
AUTHORISED	PAYMENT	Invoice & Mandate	£40.1m	£28.6m	£27.1m	£29.6m	£25.5m	£24.0m	£24.8m	£25.4m	£25.7m	**4%**
AUTHORISED	PAYMENT	CEO	£2.4m	£2.4m	£6.1m	£6.6m	£7.9m	£5.6m	£6.9m	£4.7m	£7.8m	**13%**
AUTHORISED	PAYMENT	IMP: Police/Bank	£34.7m	£56.1m	£75.6m	£61.8m	£59.4m	£50.4m	£43.5m	£35.4m	£32.3m	**-26%**
AUTHORISED	PAYMENT	IMP: Other	£22.5m	£33.3m	£43.0m	£34.6m	£30.8m	£37.0m	£32.6m	£24.7m	£18.8m	**-42%**
AUTHORISED	PAYMENT	Purchase	£23.9m	£27.2m	£32.3m	£31.8m	£31.1m	£35.9m	£40.9m	£45.1m	£42.3m	**3%**
AUTHORISED	PAYMENT	Investment	£47.6m	£61.8m	£90.6m	£81.1m	£58.4m	£55.7m	£57.2m	£50.7m	£56.4m	**-1%**
AUTHORISED	PAYMENT	Romance	£8.5m	£9.3m	£12.7m	£18.2m	£14.6m	£16.7m	£18.5m	£18.1m	£14.5m	**-21%**
AUTHORISED	PAYMENT	Advance Fee	£8.3m	£13.9m	£14.1m	£18.1m	£14.2m	£18.0m	£15.1m	£16.3m	£15.8m	**5%**