UK Finance

Half Year Fraud Report 2025

In partnership with

BioCatch
Stay Safe.

Contents

Foreword UK Finance

Fraud is a major threat to our society, our economy and continues to be the most common crime in UK today, accounting for over 40 per cent of all reported crime. This figure barely scratches the surface, as fraud is underreported meaning the true scale is far greater. Most of us have encountered fraudulent messages on social media, via email, or by text; and many have either been defrauded or have a loved one who has.

The financial losses are significant, and the criminals who perpetrate these crimes are damaging our economy and undermining the UK's growth agenda every single day. The organised crime groups responsible for committing these crimes make huge profits, which in turns enables them to grow stronger and commit other crimes which cause further individual, societal, and economic harm. The scale of the threat is not commensurate with the current level of government investment in countering it or the insufficient action by other sectors. More needs to be done to prevent this dreadful crime.

But fraud is not just a financial crime; it is a human one. The psychological harm caused by fraud, particularly the types of fraud that involve the manipulation and exploitation of the victim online or over the telephone, can be severe. Tragically, there are far too many cases of suicide where being a victim of fraud is believed to be a contributing factor.

We are just over a year into the new mandatory reimbursement system being in place. It has led to an increase in the amount of stolen money being reimbursed, but on its own does nothing to prevent the psychological harm to victims. Nor does it do anything to prevent serious organised crime groups from becoming even more dangerous.

The financial services industry invests more than any other sector in fighting fraud. Initiatives such as the Banking Protocol, where branch staff work with police to stop vulnerable people being scammed, has prevented over £400million being stolen. We also fund the Dedicated Fraud and Payment Crime Unit, a police unit which has prevented over £63 million from being stolen this year alone.

Preventing fraud is key and after continued efforts and investment we have seen a 21 per cent increase in prevented card fraud in the first half of this year. The £682 million which was stopped from being stolen is the highest ever figure reported. However, despite these efforts, as the headlines of this report show, the financial services industry cannot tackle this threat alone.

The majority of fraud originates on social media and telecommunications channels, with manipulation beginning long before any payment is made. By the time the bank has any chance in identifying it as fraud, there has often already been extensive contact with the victim on social media or other platforms which is invisible to our sector.

We need true cross-sector collaboration. Anyone whose platforms are exploited by fraudsters has a moral obligation to protect people from these crimes, and the government must hold the social media and telecommunications industries properly to account.

Fraud is not inevitable, the government needs to do much more as the scale of fraud is a national threat, one that impacts our economy and public trust. What we need is a robust Fraud Strategy: one that prioritises prevention and outcomes, holds all sectors whose platforms are exploited to account and provides the strategic leadership necessary to protect people and our economy.

Ben Donaldson

Managing Director, Economic Crime

Drivers behind the figures

UK Finance data for the first half of 2025 shows an increase in both the total number of fraud cases and the amount of money lost to fraud and scams compared with the same period in 2024. A total of £629.3 million was stolen by criminals in the first six months of this year, and there were 2.09 million confirmed cases across both authorised and unauthorised fraud. This represents a three per cent increase in losses and a 17 per cent increase in cases relative to the first half of 2024.

The trends underlying the data are slightly different from that reported last year, and in our report covering 2024 as a whole, when we saw declining authorised payment fraud replaced with rising levels of unauthorised fraud.

In the first six months of 2025 rising case numbers continue to come from higher incidences of unauthorised fraud, while higher losses can be attributed to larger amounts being stolen through authorised payment fraud.

Looking first at the detail of unauthorised fraud, which includes cards, cheques, and remote banking. Overall fraud losses via these channels were three per cent lower in the first half of 2025 compared with 2024, with more significant declines reported in cheque fraud losses (41 per cent lower than 2024 H1) and remote banking losses (down nearly a quarter).

In contrast, our data indicates a five per cent increase in card fraud to £299 million. This type of fraud was also a significant driver of overall cases. There were 1.94 million unauthorised card fraud cases in H1, nearly a fifth up on a year ago; the highest ever recorded total for a six-month period.

This increase hasn't just occurred in the most recent period, however; card fraud losses and cases have been on a steady upward trajectory since the first half of 2023. And within this remote purchase, or card not present fraud (CNP), is a key factor behind the increase. In 2025 H1 CNP cases rose 22 per cent to 1.65 million and accounted for 58 per cent of all unauthorised fraud losses, indeed this equates to more fraud than all categories of card fraud combined for any H1 period prior to 2024.

Discussions with industry highlight the ongoing challenge from social engineering and compromised one-time passcodes (OTPs), which can allow criminals to register digital wallets and make fraudulent transactions. While case volumes have surged, average case values have been declining. This points to security systems identifying vulnerabilities earlier, but it also requires criminals to target ever-increasing numbers of people. The scale of attack levels is further demonstrated by the 21 per cent increase in prevented card fraud, and at £682 million just in the first half this year, this is also the highest figure reported, and equivalent to more than twice the value stolen by criminals.

Across other types of card fraud cases and losses are considerably lower compared with remote purchase fraud, and year-on-year changes were more limited. In the second largest category, lost and stolen cards, losses were broadly unchanged from 2024 H1 with a modest five per cent increase in cases. This is in line with the steady increase in the overall number of credit and debit cards in issue in recent years. We also saw an increase in contactless fraud in the first six months of 2025, up 27 per cent on a year ago. Nevertheless, the fraud rate on contactless cards was 1.2p per £100 of transactions, significantly lower than the rate across all types of card fraud (6.9p per £100).

Elsewhere in unauthorised fraud, remote banking losses, which includes telephone, online, and mobile banking, dropped by 24 per cent to £70.7 million in H1 compared with H1 2024. Within this there were substantial falls in losses via online and telephone banking.

Losses across these two channels were the lowest ever reported for a six-month period in 2025 H1 – a consequence of both the ongoing security enhancements across all remote banking channels, but more likely a result of declining consumer use of telephone and internet banking. UK Finance's UK Payment Markets Report 2025 showed telephone banking has been declining steadily since 2020, but there has been a more material migration away from online banking in 2023 and 2024, towards mobile banking, which is now the main form of access to banking services with 75 per cent of UK adults being users. And across mobile banking we also saw an uplift in fraud cases and losses in H1 2025 (eight per cent and nine per cent respectively).

Turning to authorised push payment fraud (APP), the trends are a mirror image of that observed across unauthorised fraud. In the first six months of this year there has been a further decline in cases (down eight per cent on a year ago), but a 12 per cent rise in losses.

Looking across the different categories of APP fraud captured in our data, the significant driver of increased APP losses was investment fraud. Losses in this category in H1 2025 were 55 per cent up on the same period a year ago and account for 38% of total APP losses. Moreover, the average loss in an investment scam case is more than 20 times that of a purchase scam – still the most common APP fraud in terms of case numbers.

However, it should be noted that we saw increased investment fraud losses emerge through 2024, particularly in the second half of last year.

Two factors have driven the rise in investment losses over the past year. Firstly, as noted above these cases involve larger amounts of money and the nature of the crime means that it can take time for individuals to realise they have been a victim and for cases to be fully investigated and closed (the point at which we record the fraud in our data). Therefore, some of the losses reported in the past 12 months relate to cases that were initiated prior to that.

However, investment scams remain a target for criminals. As we reported in our full-year Fraud Report, industry intelligence also points to an ongoing prevalence of scams related to cryptocurrencies and the promise of significant returns advertised on social media. This is also a key focus for industry prevention efforts and re-enforce the need for ongoing awareness raising the risks from such scams.

Also concerning is the rise in romance scam cases and losses over the past 12 months (up 19 per cent and 35 per cent respectively). This is a particularly pernicious crime, leading to not only financial loss, but psychological harm to the victim. It is key that education and awareness efforts highlighting particular risks from romance and investment fraud continue to take centre stage. This cannot rely solely on the banking and payments

industry, as our data on APP fraud enabler continue to show most cases (around two-thirds) start online.

Education campaigns around impersonation fraud do appear to be continuing to drive down these types of scams, with losses and cases relating to the impersonation of police or bank officials, and other forms of impersonation dropping to series lows in the first half of this year.

The Payment Systems Regulator has now published nine months of data on the performance of mandatory reimbursement on APP fraud, and it shows a consistent reimbursement rate of nearly 90 per cent – in line with expectations from the industry and the regulator. This is positive for victims of fraud but still means that millions of pounds are ending up in the pockets of criminals.

Our data highlights the evolution and adaptability of fraudsters' tactics, which is causing harm to a growing number of victims in each reporting period and funnelling significant sums of money to criminal enterprises. The rising value of prevented fraud resulting from the prioritisation of industry investment in detection and consumer awareness is against an ever rising tide of attack levels that demands the forthcoming government fraud strategy brings together action from the industry, tech and telecoms companies and law enforcement to reduce the number of victims of fraud.

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) 2025 vs H1 (Jan to June) 2024 unless otherwise stated

Fraud in the first half of 2025

£629M

stolen through fraud in the first half of 2025

2.1M

confirmed cases, 17 per cent more than in 2024

£870M

of unauthorised fraud prevented by industry, 20 per cent than in 2024 and equivalent to 70p in every £1 attempted.

Losses

The total value of gross losses (unauthorised and authorised)

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Unauthorised	£374.0m	£409.8m	£397.3m	£333.0m	£352.4m	£374.5m	£341.2m	£367.6m	£381.4m	£393.3m	£371.8m	**-3%**
Authorised	£188.1m	£232.6m	£301.5m	£281.8m	£241.9m	£243.3m	£239.3m	£220.4m	£229.8m	£254.2m	£257.5m	**12%**
Total	£562.2m	£642.4m	£698.8m	£614.8m	£594.3m	£617.8m	£580.5m	£587.9m	£611.2m	£647.5m	£629.3m	**3%**

Cases

The total number of confirmed cases (where a loss has occurred)

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Unauthorised	1,383,352	1,527,157	1,496,840	1,415,627	1,397,765	1,383,546	1,264,275	1,465,532	1,670,478	1,812,930	1,981,997	**19%**
Authorised	69,093	85,521	101,540	94,456	95,167	112,205	116,316	116,111	120,184	111,290	110,747	**-8%**
Total	1,452,445	1,612,678	1,598,380	1,510,083	1,492,932	1,495,751	1,380,591	1,581,643	1,790,662	1,924,220	2,092,744	**17%**

Total unauthorised fraud

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

Unauthorised fraud losses were **£372 million** in the first six months of 2025, a decrease of three per cent from the same period in 2024.

There were **1.98 million** confirmed cases of unauthorised fraud reported in H1 2025, a 19 per cent rise on the total reported in H1 2024.

The industry prevented a further **£870million** of unauthorised fraud – equivalent to 70p in every £1 of attempted unauthorised fraud being stopped without a loss occurring.

Cards

Prevented: **£682.2m** (+21%)
Losses: **£298.9m** (+5%)
Cases: **1.94m** (+19%)

Cheques

Prevented: **£54.7m** (+359%)
Losses: **£2.2m** (-41%)
Case: **335** (-47%)

Remote Banking

Prevented: **£132.8m** (-11%)
Losses: **£70.7m** (-24%)
Case: **41,746** (+5%)

Total unauthorised card fraud

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Prevented	£486.8m	£496.5m	£481.7m	£484.9m	£492.0m	£482.2m	£519.5m	£502.2m	£564.4m	£623.6m	£682.2m	**21%**
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	1,630,264	1,773,813	1,939,916	**19%**
Gross Loss	£287.9m	£286.4m	£261.3m	£263.2m	£270.2m	£286.0m	£260.0m	£291.4m	£285.0m	£306.2m	£298.9m	**5%**

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

Remote purchase (Card not present), Lost & Stolen, Card not received, Counterfeit card and Card ID theft

Fraud losses on cards totalled £298.9 million in the first half of 2025, an increase of five per cent on the same period in 2024.

Over this period the overall value of card spending by UK cardholders fell slightly. Card fraud as a proportion of card purchases has increased from 6.8p in the first half of 2024 to 6.9p in the first half of 2025. A total of £682.2 million of card fraud was stopped by banks and card companies in the first six months of 2025. This is equivalent to £6.95 in every £10 of attempted card fraud prevented without a loss occurring.

Remote purchase (Card Not Present)

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 202	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	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	1,355,054	1,470,289	1,655,112	**22%**
Gross Loss	£222.8m	£229.8m	£210.1m	£202.4m	£198.1m	£197.6m	£174.5m	£186.0m	£199.6m	£211.7m	£215.4m	**8%**

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 eight per cent to £215.4 million in the first six months of 2025. The number of cases increased by 22 per cent to 1.66 million.

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 £159 million in the first half of 2025, an increase of nine per cent when compared with the same period in 2024.

Lost and Stolen

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Cases	166,710	155,284	144,713	180,788	185,609	215,731	188,409	209,140	209,127	231,902	220,071	**5%**
Gross Loss	£41.1m	£37.8m	£35.1m	£42.1m	£46.9m	£53.2m	£48.6m	£55.4m	£51.5m	£59.9m	£51.9m	**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.

Losses due to lost and stolen card fraud increased by one per cent in H1 2025 and totalled £51.9 million. The number of incidents reported increased five per cent to just over 220,000 cases.

Card Not Received

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Cases	4,193	4,242	4,126	4,815	5,093	3,755	2,874	3,059	3,541	3,857	3,914	**11%**
Gross Loss	£2.1m	£2.3m	£2.0m	£2.0m	£1.9m	£2.0m	£1.4m	£1.6m	£1.9m	£1.0m	£1.3m	**-30%**

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 decreased by 30 per cent to £1.3 million during January to June 2025, case volumes increased by 11% 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

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Cases	28,389	24,393	14,640	10,268	9,664	9,930	8,633	9,437	7,605	7,378	8,539	**12%**
Gross Loss	£5.4m	£3.3m	£2.6m	£2.1m	£2.2m	£2.5m	£2.3m	£2.4m	£2.1m	£1.8m	£2.3m	**8%**

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

Counterfeit card losses totalled £2.3 million in H1 2025, a rise of eight per cent on the total reported in 2024. Case volumes rose by 12 per cent to 8,539. Looking over a longer time horizon cases and losses from counterfeit cards remains fairly static.

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

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Cases	18,955	15,590	16,955	23,071	34,217	47,847	61,249	81,196	54,937	60,387	52,280	**-5%**
Gross Loss	£16.5m	£13.2m	£11.5m	£14.7m	£21.1m	£30.6m	£33.1m	£46.0m	£29.8m	£31.7m	£28.0m	**-6%**

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 six per cent in the first six months of 2025 compared with the same period in 2024, from £29.8 million to £28.0 million. The number of individual cases also decreased over the same period, dropping by 5% to 52,280 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

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

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
UK Retail	£25.5m	£23.3m	£19.6m	£27.3m	£33.3m	£38.8m	£38.4m	£50.3m	£38.0m	£47.3m	£40.0m	5%

UK retail face-to-face card fraud covers all transactions that occur in person in a UK shop including contactless. Much of this fraud is undertaken using low-tech techniques, with fraudsters finding ways of stealing the card, and often the PIN, to carry out fraudulent transactions in shops. This includes criminals using methods such as ATM card entrapment and distraction thefts, combined with shoulder surfing and PIN pad cameras. Criminals also use various social engineering methods to dupe victims into handing over their cards on their own front doorstep, often known as courier scams.

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

UK Internet / E-Commerce Fraud

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
UK ECOM	£117.0m	£125.9m	£121.9m	£114.2m	£111.3m	£109.2m	£97.4m	£105.0m	£112.7m	£118.2m	£122.6m	9%

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

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

UK Cash Machine Fraud

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
UK ATM	£15.0m	£13.1m	£12.0m	£12.4m	£12.9m	£13.2m	£12.7m	£12.9m	£12.8m	£13.0m	£12.8m	0%

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 are unchanged in the first half of 2025. Most of this fraud is thought to be perpetuated through distraction thefts and card entrapment at ATMs.

UK / International Card Fraud

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
UK	£208.5m	£206.0m	£187.6m	£196.4m	£202.4m	£213.8m	£197.2m	£219.7m	£204.8m	£223.6m	£221.3m	8%
INT	£79.4m	£80.4m	£73.7m	£66.8m	£67.9m	£72.2m	£62.8m	£71.7m	£80.2m	£82.6m	£77.6m	-3%

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.

UK card fraud losses increased by eight per cent to £221.3 million and international fraud losses decreased by three per cent, to £77.6 million.

Unauthorised Cheque Fraud

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Prevented	£184.2m	£54.3m	£21.0m	£12.0m	£10.5m	£9.3m	£7.3m	£5.0m	£11.9m	£41.8m	£54.7m	**359%**
Cases	709	538	382	433	415	551	559	638	636	470	335	**-47%**
Gross Loss	£6.4m	£5.8m	£3.5m	£2.9m	£3.2m	£4.3m	£2.9m	£2.8m	£3.8m	£4.3m	£2.2m	**-41%**

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 decreased by 41 per cent in the first half of 2025, while the number of cases fell 47 per cent to 335 cases. Both figures are the lowest ever reported for a six-month period in the category.

Unauthorised Remote Banking

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Prevented	£181.5m	£212.3m	£230.3m	£135.3m	£88.1m	£86.0m	£104.6m	£113.5m	£149.3m	£116.2m	£132.8m	**-11%**
Cases	29,997	43,643	51,462	36,988	25,881	21,592	18,492	18,920	39,578	38,647	41,746	**5%**
Gross Loss	£79.7m	£117.6m	£132.5m	£67.0m	£78.9m	£84.2m	£78.3m	£73.4m	£92.6m	£82.7m	£70.7m	**-24%**

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 £70.7 million in the first half of 2025, a 24 per cent decrease compared with the amount lost in the first six months 2024. The number of cases of remote banking fraud increased by 5 per cent to 41,746.

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 £132.8 million of attempted remote banking fraud was stopped by bank security systems in the first six months of 2025. This is equivalent to 65p in every £1 of fraud attempted being prevented.

In addition, 7 per cent (£5.3 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.

Unauthorised Internet Banking

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Cases	21,312	34,683	42,628	29,929	18,001	14,035	7,775	5,894	4,744	4,432	4,771	**1%**
Gross Loss	£64.3m	£95.4m	£108.0m	£50.3m	£55.5m	£58.6m	£50.5m	£38.2m	£44.2m	£33.6m	£24.0m	**-46%**

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 2025, falling 46 per cent to £24.0 million when compared with the same period in 2024. Case volumes increased slightly, rising one per cent to 4,771 cases.

Unauthorised Telephone Banking

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Cases	4,681	2,809	2,545	2,078	1,776	1,300	1,533	2,178	1,723	2,010	1,314	**-24%**
Gross Loss	£7.9m	£8.1m	£7.5m	£8.0m	£7.4m	£7.3m	£7.3m	£10.3m	£8.8m	£7.9m	£3.7m	**-58%**

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 decreased by 58 per cent to £3.7 million in the first six months of 2025. The number of cases decreased by 24 per cent to 1,314; both the lowest totals ever reported for a six month period.

Unauthorised Mobile Banking

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Cases	4,004	6,151	6,289	4,981	6,104	6,257	9,184	10,848	33,111	32,205	35,661	**8%**
Gross Loss	£7.5m	£14.0m	£17.1m	£8.7m	£16.0m	£18.2m	£20.6m	£24.9m	£39.6m	£41.2m	£43.0m	**9%**

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 75 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 nine per cent to £43.0 million in the first six months of 2025, 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 eight per cent to 35,661; another record high for the first half of the year.

Authorised Push Payment (APP)

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Cases	69,093	85,521	101,540	94,456	95,167	112,205	116,316	116,111	120,184	111,290	110,747	**-8%**
Payments	105,069	139,502	172,622	172,515	166,327	205,939	211,560	205,900	217,238	210,941	226,306	**4%**
Gross Loss	£188.1m	£232.6m	£301.5m	£281.8m	£241.9m	£243.3m	£239.3m	£220.4m	£229.8m	£254.2m	£257.5m	**12%**
Returned to Victim	£75.0m	£99.7m	£125.8m	£131.9m	£135.6m	£150.0m	£152.8m	£134.5m	£128.5m	£143.2m	£159.2m	**24%**

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.

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:

- 66% of fraud cases are enabled by online sources. These cases tend to include lower-value scams such as purchase fraud and therefore account for 30% of total losses.
- 17% of fraud cases are enabled by telecommunications, these are usually higher value cases such as impersonation scams and so account for 29% 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.

	H1 2024		H1 2025	
	Value	Volume	Value	Volume
Online	32%	71%	30%	66%
Telecommunications	35%	16%	29%	17%
Email	10%	1%	9%	1%
Other	6%	3%	8%	5%
Unknown	17%	8%	24%	11%

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.

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.

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

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

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

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

Purchase Scam

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Cases	40,486	43,806	50,327	49,406	53,907	63,263	76,943	79,573	86,087	80,711	80,128	-7%
Payments	50,933	56,560	64,948	67,463	72,282	86,836	107,655	111,939	122,529	117,262	118,104	-4%
Loss	£23.9m	£27.2m	£32.3m	£31.8m	£31.1m	£35.9m	£40.9m	£45.1m	£48.1m	£50.6m	£53.0m	10%
Returned to Victim	£6.5m	£8.1m	£9.3m	£11.7m	£16.5m	£21.6m	£25.7m	£30.1m	£28.8m	£31.9m	£39.6m	38%

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 80,128 confirmed cases accounting for 72 per cent of the total number of all APP scam cases reported in the first half of 2025. A total of £53.0 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 £39.6 million (75%) of the losses to the victims.

Investment Scam

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Cases	3,655	4,526	6,224	5,850	5,161	4,924	5,112	5,114	5,660	6,149	6,471	14%
Payments	8,720	11,203	17,567	18,098	14,928	15,583	16,942	16,454	19,072	22,514	25,156	32%
Loss	£47.6m	£61.8m	£90.6m	£81.1m	£58.4m	£55.7m	£57.2m	£50.7m	£63.0m	£95.1m	£97.7m	55%
Returned to Victim	£14.2m	£22.6m	£34.8m	£37.0m	£29.4m	£29.2m	£33.5m	£25.5m	£30.5m	£42.8m	£47.3m	55%

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 increased by 55 per cent in January to June 2024 to £97.7million. Investment scams continued to account for the largest value of all eight APP scam types accounting for 38 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 six per cent of the total number of APP scam cases. It should also be noted that investment scams typically take a while for the investor to realise they have been a victim of a scam, so whilst losses have increased in the current period, the actual payment to the scammer will most likely have occurred some time ago.

Payment service providers returned £47.3 million (48 per cent) of the losses to the victims.

Romance Scam

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Cases	1,107	1,218	1,479	1,791	1,644	2,005	2,120	2,040	2,527	2,683	2,995	**19%**
Payments	6,051	7,134	11,489	14,325	13,199	17,021	18,889	20,689	23,392	25,884	27,766	**19%**
Loss	£8.5m	£9.3m	£12.7m	£18.2m	£14.6m	£16.7m	£18.5m	£18.1m	£15.2m	£16.6m	£20.5m	**35%**
Returned to Victim	£2.9m	£3.1m	£4.3m	£7.8m	£7.2m	£9.3m	£11.6m	£11.2m	£9.6m	£10.2m	£12.6m	**31%**

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 £20.5 million was lost to romance scams during January to June 2025, an increase of 35 per cent when compared with the same period in 2024. Romance scams have an average of over nine 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 £12.6 million to victims or 61 per cent of the total.

Advance Fee Scam

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Cases	5,697	8,136	9,064	11,431	11,472	15,857	12,238	11,610	9,933	7,527	7,574	**-24%**
Payments	9,245	13,987	16,233	20,737	20,609	30,622	27,047	23,912	21,669	19,085	27,659	**28%**
Loss	£8.3m	£13.9m	£14.1m	£18.1m	£14.2m	£18.0m	£15.1m	£16.3m	£17.1m	£18.2m	£19.6m	**14%**
Returned to Victim	£3.0m	£4.5m	£5.3m	£6.1m	£6.3m	£11.5m	£9.6m	£11.7m	£10.6m	£9.7m	£13.1m	**24%**

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 2025, accounting for seven per cent of the total number of cases.

A total of £19.6 million was lost to advance fee scams, an increase of 14 percent compared with the first six months of 2024. Payment service providers returned £13.1million (67 per cent) of the losses to the victims.

Invoice and Mandate Scam

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Cases	2,778	1,943	2,053	2,277	1,591	1,749	1,665	1,445	1,168	1,193	1,170	**0%**
Payments	3,613	2,707	2,813	3,354	2,340	2,625	2,352	2,060	1,649	1,749	1,913	**16%**
Loss	£40.1m	£28.6m	£27.1m	£29.6m	£25.5m	£24.0m	£24.8m	£25.4m	£26.0m	£17.1m	£19.9m	**-24%**
Returned to Victim	£16.5m	£13.3m	£10.8m	£11.7m	£13.6m	£12.8m	£12.2m	£11.4m	£11.9m	£9.2m	£9.2m	**-23%**

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 £19.9 million in the first half of 2025, a decrease of 24 per cent when compared with the same period in 2024. 75 per cent (£15 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 £9.2 million (46 per cent) of the losses to the victims.

CEO Scam

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Cases	187	170	230	231	200	232	196	215	157	120	78	**-50%**
Payments	235	252	331	347	297	318	302	289	287	165	106	**-63%**
Loss	£2.4m	£2.4m	£6.1m	£6.6m	£7.9m	£5.6m	£6.9m	£4.7m	£7.8m	£4.1m	£1.6m	**-79%**
Returned to Victim	£1.1m	£0.7m	£1.6m	£1.2m	£2.2m	£1.4m	£1.4m	£1.7m	£1.3m	£1.0m	£0.3m	**-73%**

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 2025, accounting for less than one per cent of total cases. A total of £1.6 million was lost, also, equivalent to less than one per cent of total APP losses. CEO has the highest average case value of all eight scam types with an average of just over £20,000 being lost per confirmed case.

Payment service providers returned £0.3 million (22 per cent) of the losses to the victims up from 17 per cent in the first half of 2024.

Impersonation: Police/Bank Staff

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Cases	7,983	13,194	17,521	11,885	9,138	7,810	5,976	4,618	4,383	3,406	3,158	-28%
Payments	14,049	26,548	34,774	28,032	22,533	25,997	17,910	12,842	11,834	8,997	10,196	-14%
Loss	£34.7m	£56.1m	£75.6m	£61.8m	£59.4m	£50.4m	£43.5m	£35.4m	£33.2m	£34.6m	£27.1m	-18%
Returned to Victim	£20.0m	£32.1m	£40.6m	£38.6m	£42.0m	£40.4m	£35.0m	£26.4m	£22.3m	£25.0m	£22.3m	0%

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 11 per cent of all APP scam losses in H1 2025 totalling £27.1 million. However, losses have decreased by 18 per cent when compared with the same period in 2024 and case volumes have fallen by 28 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 £22.3 million of the losses to victims.

Impersonation: Other

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Cases	7,200	12,528	14,642	11,585	12,054	16,365	12,066	11,496	10,269	9,501	9,173	-11%
Payments	12,223	21,111	24,467	20,159	20,139	26,937	20,463	17,715	16,806	15,285	15,406	-8%
Loss	£22.5m	£33.3m	£43.0m	£34.6m	£30.8m	£37.0m	£32.6m	£24.7m	£19.3m	£17.9m	£18.0m	-7%
Returned to Victim	£10.8m	£15.3m	£19.2m	£17.7m	£18.5m	£23.8m	£23.9m	£16.5m	£13.5m	£13.5m	£14.8m	10%

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 £18.0 million was lost to this type of scam during the first six months of 2025, a decrease of seven per cent when compared with 2024.

Payment service providers were able to return £14.8million of the losses to customers or 82 per cent of the total.

APP: 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 Values	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Faster Payment	£149.3m	£200.1m	£263.7m	£240.8m	£208.3m	£212.8m	£199.1m	£181.1m	£175.8m	£208.5m	£208.9m	**19%**
CHAPS	£8.2m	£6.3m	£9.3m	£13.2m	£8.8m	£5.1m	£13.1m	£10.0m	£11.6m	£4.3m	£6.1m	**-47%**
BACS	£15.1m	£8.4m	£11.1m	£9.3m	£12.5m	£11.4m	£13.2m	£14.6m	£20.2m	£7.0m	£8.4m	**-58%**
Intra Bank Transfer ("on us")	£2.7m	£7.9m	£5.3m	£2.3m	£0.5m	£1.1m	£1.6m	£1.0m	£3.2m	£3.5m	£4.2m	**32%**
International	£12.9m	£9.9m	£12.2m	£16.2m	£11.8m	£12.9m	£12.3m	£13.6m	£19.0m	£30.9m	£29.8m	**57%**
Total	£188.1m	£232.6m	£301.5m	£281.8m	£241.9m	£243.3m	£239.3m	£220.4m	£229.8m	£254.2m	£257.5m	**12%**

Payment Type Volumes	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Faster Payment	101,297	135,344	167,720	167,731	163,142	201,822	207,959	201,574	211,867	203,011	213,525	**1%**
CHAPS	244	257	435	329	398	152	196	253	144	172	78	**-46%**
BACS	667	526	729	966	911	1,316	1,284	1,246	1,073	1,061	1,333	**24%**
Intra Bank Transfer ("on us")	1,402	1,711	2,100	1,258	532	710	812	834	1,872	2,996	6,421	**243%**
International	1,459	1,664	1,638	2,231	1,344	1,939	1,309	1,993	2,282	3,701	4,949	**117%**
Total	105,069	139,502	172,622	172,515	166,327	205,939	211,560	205,900	217,238	210,941	226,306	**4%**

APP: Payment Channel

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

Payment Channel Values	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Branch	£19.7m	£23.9m	£27.2m	£29.3m	£25.0m	£20.7m	£27.5m	£22.5m	£22.9m	£17.2m	£18.4m	**-20%**
Internet Banking	£126.8m	£135.7m	£171.4m	£157.7m	£135.6m	£139.0m	£129.5m	£95.4m	£96.1m	£91.0m	£104.6m	**9%**
Telephone Banking	£9.7m	£8.1m	£11.3m	£13.1m	£8.7m	£6.9m	£7.7m	£11.2m	£8.7m	£12.1m	£7.4m	**-15%**
Mobile Banking	£32.0m	£64.8m	£91.5m	£81.7m	£72.5m	£76.8m	£74.7m	£91.2m	£102.0m	£133.9m	£127.0m	**25%**
Total	£188.1m	£232.6m	£301.5m	£281.8m	£241.9m	£243.3m	£239.3m	£220.4m	£229.8m	£254.2m	£257.5m	**12%**

Payment Channel Volumes	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Branch	3,445	5,523	4,070	4,181	3,754	4,811	4,480	3,695	2,820	2,754	2,942	**4%**
Internet Banking	55,608	58,245	62,789	67,227	63,229	75,471	72,370	51,087	40,237	40,024	46,063	**14%**
Telephone Banking	2,687	2,906	2,725	3,524	3,203	2,973	3,710	2,908	1,549	1,635	1,723	**11%**
Mobile Banking	43,329	72,828	103,038	97,583	96,141	122,668	131,000	148,209	172,632	166,528	175,578	**2%**
Total	105,069	139,502	172,622	172,515	166,327	205,939	211,560	205,900	217,238	210,941	226,306	**4%**

Our Fraud Data

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

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

Some caveats are required for the tables in the document.

- Prevented values were not collected for all fraud types prior to 2015.
- The sum of components may not equal the total due to rounding. .
- Data series are subject to restatement, based on corrections or the receipt of additional information.

Methodology for Data Collection

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

Validation check

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

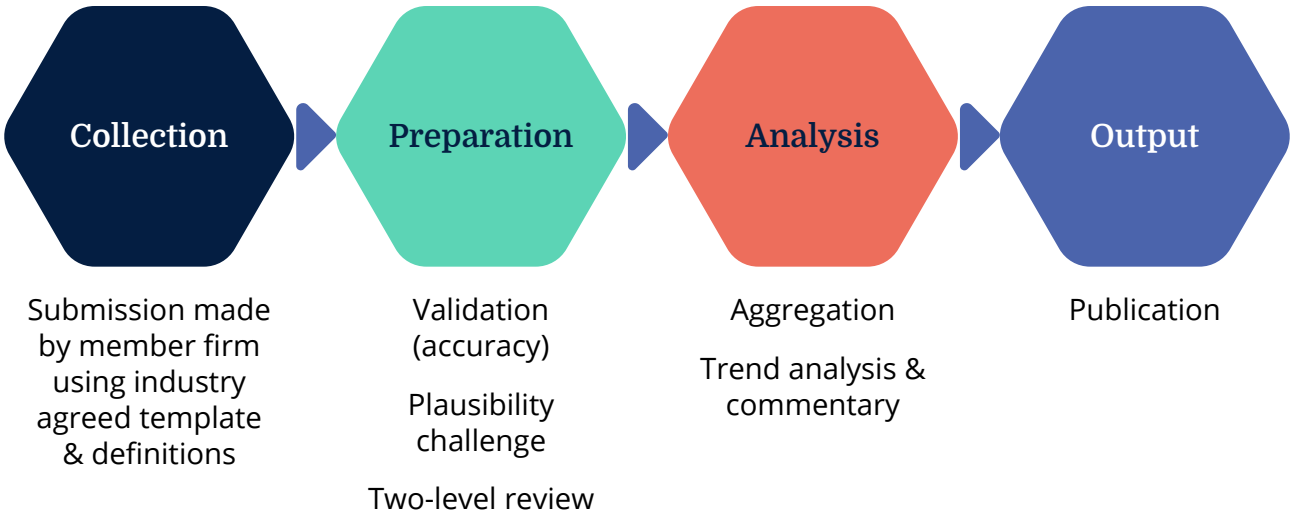
Data plausibility - inputs

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

Data plausibility – outputs

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

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



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

Contributing Members

Allied Irish Bank
American Express
Arbuthnot Latham & Co
Bank Of Ireland
Barclays Bank
C Hoare & Co.
Capital One
Co-operative Bank
Coventry Buidling Society
Danske Bank
Hampden & Co
HSBC
Investec
Lloyds Banking Group
Marks & Spencer
Metro Bank
Modulr
Monzo
Nationwide
Newday
Natwest Group
Sainsbury's Bank
Santander
Starling Bank
Silicon Valley Bank (HSBC Innovation)
Tesco Bank
Triodos Bank
TSB
Vanquis
Virgin Money
Weatherbys Bank
Yorkshire Bank
Zopa

Appendix

Cases

Type	Category	Sub Category	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Unauthorised	**Card**	**Lost & stolen**	166,710	155,284	144,713	180,788	185,609	215,731	188,409	209,140	209,127	231,902	220,071	**5%**
Unauthorised	**Card**	**CNR**	4,193	4,242	4,126	4,815	5,093	3,755	2,874	3,059	3,541	3,857	3,914	**11%**
Unauthorised	**Card**	**Counterfeit**	28,389	24,393	14,640	10,268	9,664	9,930	8,633	9,437	7,605	7,378	8,539	**12%**
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	1,355,054	1,470,289	1,655,112	**22%**
Unauthorised	**Card**	**Card ID Theft**	18,955	15,590	16,955	23,071	34,217	47,847	61,249	81,196	54,937	60,387	52,280	**-5%**
Unauthorised	**Cheque**	**Cheque**	709	538	382	433	415	551	559	638	636	470	335	**-47%**
Unauthorised	**Remote Banking**	**Internet Banking**	21,312	34,683	42,628	29,929	18,001	14,035	7,775	5,894	4,744	4,432	4,771	**1%**
Unauthorised	**Remote Banking**	**Telephone Banking**	4,681	2,809	2,545	2,078	1,776	1,300	1,533	2,178	1,723	2,010	1,314	**-24%**
Unauthorised	**Remote Banking**	**Mobile Banking**	4,004	6,151	6,289	4,981	6,104	6,257	9,184	10,848	33,111	32,205	35,661	**8%**
Authorised	**Payment**	**Invoice & Mandate**	3,613	2,707	2,813	3,354	2,340	2,625	2,352	2,060	1,649	1,749	1,913	**16%**
Authorised	**Payment**	**CEO**	235	252	331	347	297	318	302	289	287	165	106	**-63%**
Authorised	**Payment**	**IMP: Police/Bank**	14,049	26,548	34,774	28,032	22,533	25,997	17,910	12,842	11,834	8,997	10,196	**-14%**
Authorised	**Payment**	**IMP: Other**	12,223	21,111	24,467	20,159	20,139	26,937	20,463	17,715	16,806	15,285	15,406	**-8%**
Authorised	**Payment**	**Purchase**	50,933	56,560	64,948	67,463	72,282	86,836	107,655	111,939	122,529	117,262	118,104	**-4%**
Authorised	**Payment**	**Investment**	8,720	11,203	17,567	18,098	14,928	15,583	16,942	16,454	19,072	22,514	25,156	**32%**
Authorised	**Payment**	**Romance**	6,051	7,134	11,489	14,325	13,199	17,021	18,889	20,689	23,392	25,884	27,766	**19%**
Authorised	**Payment**	**Advance Fee**	9,245	13,987	16,233	20,737	20,609	30,622	27,047	23,912	21,669	19,085	27,659	**28%**

Losses

Type	Category	Sub Category	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	Change
Unauthorised	Card	Lost & stolen	£41.1m	£37.8m	£35.1m	£42.1m	£46.9m	£53.2m	£48.6m	£55.4m	£51.5m	£59.9m	£51.9m	**1%**
Unauthorised	Card	CNR	£2.1m	£2.3m	£2.0m	£2.0m	£1.9m	£2.0m	£1.4m	£1.6m	£1.9m	£1.0m	£1.3m	**-30%**
Unauthorised	Card	Counterfeit	£5.4m	£3.3m	£2.6m	£2.1m	£2.2m	£2.5m	£2.3m	£2.4m	£2.1m	£1.8m	£2.3m	**8%**
Unauthorised	Card	Remote purchase	£222.8m	£229.8m	£210.1m	£202.4m	£198.1m	£197.6m	£174.5m	£186.0m	£199.6m	£211.7m	£215.4m	**8%**
Unauthorised	Card	Card ID Theft	£16.5m	£13.2m	£11.5m	£14.7m	£21.1m	£30.6m	£33.1m	£46.0m	£29.8m	£31.7m	£28.0m	**-6%**
Unauthorised	Cheque	Cheque	£6.4m	£5.8m	£3.5m	£2.9m	£3.2m	£4.3m	£2.9m	£2.8m	£3.8m	£4.3m	£2.2m	**-41%**
Unauthorised	Remote Banking	Internet Banking	£64.3m	£95.4m	£108.0m	£50.3m	£55.5m	£58.6m	£50.5m	£38.2m	£44.2m	£33.6m	£24.0m	**-46%**
Unauthorised	Remote Banking	Telephone Banking	£7.9m	£8.1m	£7.5m	£8.0m	£7.4m	£7.3m	£7.3m	£10.3m	£8.8m	£7.9m	£3.7m	**-58%**
Unauthorised	Remote Banking	Mobile Banking	£7.5m	£14.0m	£17.1m	£8.7m	£16.0m	£18.2m	£20.6m	£24.9m	£39.6m	£41.2m	£43.0m	**9%**
Authorised	Payment	Invoice & Mandate	£40.1m	£28.6m	£27.1m	£29.6m	£25.5m	£24.0m	£24.8m	£25.4m	£26.0m	£17.1m	£19.9m	**-24%**
Authorised	Payment	CEO	£2.4m	£2.4m	£6.1m	£6.6m	£7.9m	£5.6m	£6.9m	£4.7m	£7.8m	£4.1m	£1.6m	**-79%**
Authorised	Payment	IMP: Police/Bank	£34.7m	£56.1m	£75.6m	£61.8m	£59.4m	£50.4m	£43.5m	£35.4m	£33.2m	£34.6m	£27.1m	**-18%**
Authorised	Payment	IMP: Other	£22.5m	£33.3m	£43.0m	£34.6m	£30.8m	£37.0m	£32.6m	£24.7m	£19.3m	£17.9m	£18.0m	**-7%**
Authorised	Payment	Purchase	£23.9m	£27.2m	£32.3m	£31.8m	£31.1m	£35.9m	£40.9m	£45.1m	£48.1m	£50.6m	£53.0m	**10%**
Authorised	Payment	Investment	£47.6m	£61.8m	£90.6m	£81.1m	£58.4m	£55.7m	£57.2m	£50.7m	£63.0m	£95.1m	£97.7m	**55%**
Authorised	Payment	Romance	£8.5m	£9.3m	£12.7m	£18.2m	£14.6m	£16.7m	£18.5m	£18.1m	£15.2m	£16.6m	£20.5m	**35%**
Authorised	Payment	Advance Fee	£8.3m	£13.9m	£14.1m	£18.1m	£14.2m	£18.0m	£15.1m	£16.3m	£17.1m	£18.2m	£19.6m	**14%**