UK Finance

Half Year Fraud Report 2026

In partnership with

BioCatch
Stay Safe.

Nasdaq
Verafin



Contents

Foreword UK Finance 4
Drivers behind the fraud figures 6
Drivers behind the figures 7
Our fraud data 11
Fraud in the first half of 2026 12
Total unauthorised fraud 13
Total unauthorised card fraud 14
Remote Purchase (Card Not Present) 14
Lost and Stolen 15
Card Not Received 15
Counterfeit Card 15
Card ID Theft 16
Further card fraud analysis 17
UK Retail Face To Face Fraud 17
UK Internet / E-Commerce Fraud 17
UK Cash Machine Fraud 18
UK / International Card Fraud 18
Unauthorised Cheque Fraud 19
Unauthorised Remote Banking 20
Unauthorised Internet Banking 21
Unauthorised Telephone Banking 22
Unauthorised Mobile Banking 22
Authorised Push Payment (APP) 23
APP Fraud Enablers 24
The Data 24
Further Analysis Of The APP Scam Data 26
Investment Scam 28

Romance Scam 28
Advance Fee Scam 29
Invoice and Mandate Scam 29
CEO Scam 30
Impersonation: Police/Bank Staff 30
Impersonation: Other 31
APP: Payment Type 32
APP: Payment Channel 32
Our Fraud Data 33
Methodology for Data Collection 33
Appendix 35
Losses 36
Contributing Members 37

Foreword UK Finance

Fraud remains one of the most significant threats facing people, businesses and the UK economy, accounting for around 47% of all crime. Criminals continue to adapt quickly, exploiting new technologies, changing consumer behaviours and vulnerabilities across different sectors to steal money from their victims.

The figures for the first half of 2026 underline the scale and evolving pace of that challenge. £659 million was stolen during the first six months of the year, an increase of eight per cent compared with the same period in 2025. Behind these figures are individuals and businesses experiencing not only financial detriment, but often considerable emotional distress. For many victims, the impact extends far beyond the immediate financial loss, affecting confidence, wellbeing and trust in the organisations and services they rely upon. Indeed, we know this extends to the wider digital economy.

The nature of the threat is also continuing to evolve. While losses from unauthorised fraud have fallen slightly, authorised push payment (APP) fraud has increased. This changing picture reinforces an important point: when one route becomes more difficult for criminals to exploit, they will look for another.

Increasingly, fraudsters are seeking to manipulate the person making the payment. Social engineering has become an integral part of the criminal toolkit, with victims targeted through online platforms, telecommunications and other channels, well before the banking system has visibility of risk. Criminals are adept at creating convincing scenarios, impersonating trusted organisations and exploiting circumstances that appear legitimate. Emerging technologies, including AI, are enabling criminals to create sophisticated fraudulent content at scale, presenting challenges for industry, consumers and policymakers alike.

Fraud continues to originate outside the banking sector but is causing harm within it

We can see this evolution across a number of fraud types. Investment fraud continues to be a particular concern and now accounts for a significant proportion of APP fraud. Criminals are quick to exploit interest in investment opportunities and emerging or high-profile assets, using sophisticated websites, online advertising and social media to convince people that fraudulent investments are genuine. These scams can develop over long periods and can result in life-changing losses before a victim realises they have been deceived.

We are also seeing changes in purchase and advance fee scams. While lower value purchase scams remain prevalent, criminals are increasingly exploiting higher value transactions, including deposits for vehicles, holidays and other goods and services. The methods may vary, but the principle remains the same: criminals create a convincing opportunity and persuade their victim to part with money, typically under time pressure, before disappearing.

There are also indications that some forms of fraud may be changing as criminals respond to improvements in security. Card not present fraud (fraud committed online or by phone without the physical card being used) has, for example, fallen significantly. Investment by the financial services industry and improvements in the protection of customers and card details are contributing to this. At the same time, the industry is seeing evidence of criminals increasingly using social engineering in card fraud. More work is needed across schemes and regulators to establish consistent definitions and robust data so that we can better understand these changing patterns.

Against this backdrop, there are important signs of progress. The banking and finance industry continues to invest heavily in protecting customers and stopping fraud before money is stolen. In the first half of 2026, more than £800 million of unauthorised fraud was prevented through sophisticated security systems and other preventative measures. Around 70p in every £1 of attempted unauthorised fraud was stopped.

Banks also prevent substantial amounts of APP fraud through increasingly sophisticated monitoring and direct intervention, often contacting customers or delaying payments where there are signs that a scam is taking place. Not every successful intervention is captured in the reported fraud figures, meaning the amount of harm prevented, is considerably greater than recorded losses alone suggest.

While it is encouraging that more money stolen through APP fraud is being returned to victims, reimbursement should not be mistaken for success in tackling fraud. The proportion returned has increased, reflecting both mandatory reimbursement requirements and the considerable work undertaken by firms to support customers. But reimbursement alone cannot be the answer. By the time a victim needs to be reimbursed, the harm has already been done and the money is in the hands of the criminals.

Prevention must therefore remain our priority. The industry already prevents more than £1.5 billion of fraud each year, but we know that financial services cannot tackle fraud alone.

The financial services sector has an important role to play and will continue investing in fraud prevention, sharing intelligence, identifying suspicious payments and supporting victims. Many frauds & scams begin well before a customer interacts with their payment service provider (PSP), on an online platform, through a fraudulent advertisement, search result, marketplace, social media message, text or telephone call.

That is why effective action across the entire fraud ecosystem is essential.

The Government's Fraud Strategy provides an important framework for strengthening the UK's response to fraud, but delivering meaningful and lasting reductions will require coordinated action across the wider fraud ecosystem. This means stronger collaboration between financial services, technology companies, telecommunications providers, law enforcement, regulators and government, underpinned by effective intelligence sharing, robust data and clear accountability for preventing fraud at source.

Criminals will continue to innovate. Our response must evolve just as quickly.

The financial services industry remains committed to protecting customers and disrupting the criminals responsible. But reducing fraud sustainably will require every sector whose services are exploited by fraudsters to play its part.

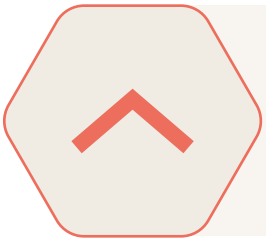
Fraud is not inevitable. Through stronger prevention, greater collaboration, intelligence sharing and coordinated action across sectors, we can make it considerably harder for criminals to reach their victims and profit from these devastating crimes.

Ruth Ray

Managing Director,
Economic Crime



Drivers behind the fraud figures



Overall fraud losses increased from
£608.9 million in 2025 H1 to
£659.5 million in 2026 H1
an increase of **8 per cent**.



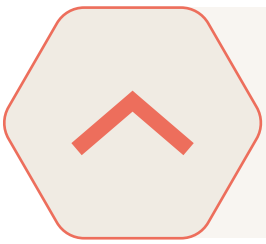
Total confirmed fraud cases fell from
2.07 million to 1.78 million
a decrease of **14.3 per cent**.



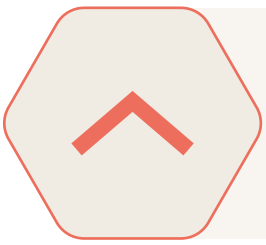
Unauthorised fraud losses fell from
£350.7 million to £343.5 million
a decrease of **2 per cent**.



Unauthorised fraud cases fell
from 1.96 million to 1.64 million
a decrease of **17 per cent**.



APP fraud losses increased from
£258.2 million to £316.0 million
a rise of **22 per cent**.



APP fraud cases increased from
110,822 to 138,345
a rise of **25 per cent**.

Drivers behind the figures

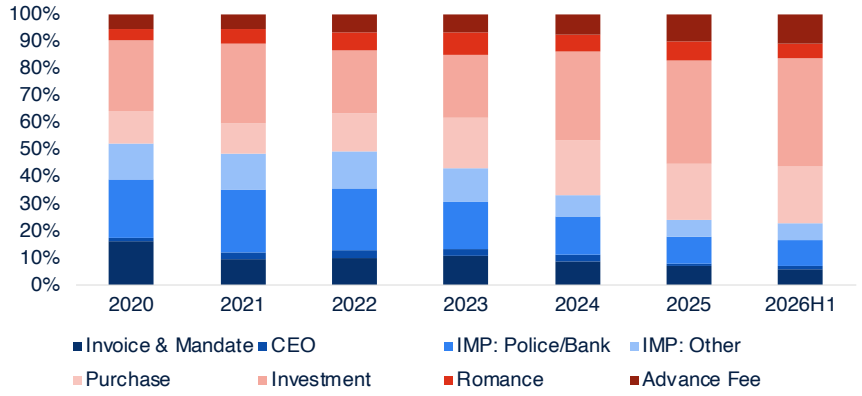
Last year we saw rising losses driven primarily by authorised push payment (APP) fraud while unauthorised fraud was broadly stable. UK Finance data for the first half of 2026 shows that divergence has become more pronounced, with another marked increase in APP fraud offsetting a modest reduction in unauthorised fraud. This represents a continued evolution in fraud patterns, with organised criminal groups adapting their tactics in response to changing consumer behaviour, stronger security controls and increased industry intervention.

A total of £659.5 million was stolen through fraud and scams in the first six months of the year, up eight per cent compared with the same period in 2025. While the total number of confirmed fraud cases fell by 14 per cent to 1.78 million, this was still the second-highest total recorded, behind last year.

Beneath these headline figures lies a markedly different story for APP fraud compared with that for unauthorised fraud. During 2025, payment service providers reported increases across both APP and unauthorised fraud. In the first half of 2026, however, the two categories moved in different directions. APP fraud was the principal driver of the increase in overall fraud losses, while unauthorised fraud fell but continued to account for the larger share of total cases and losses.

Looking first at APP fraud, the trends observed during 2025 have intensified. Losses increased by 22 per cent to £316 million while case volumes rose by 25 per cent to 138,345, both representing the highest figures recorded for a first half-year period. The continued growth in APP fraud during the first half of 2026 was driven overwhelmingly by malicious payee fraud (chart 1, orange categories) – scams which convince victims to make what they believe is a legitimate payment for goods, services or investment opportunities that do not exist. This reinforces a trend that has become increasingly evident in recent years.

Chart 1. APP losses, percentage of total by scam type



Investment scams remain the largest contributor to APP losses, accounting for around 40 per cent of all APP losses recorded during the period. Losses increased to £126.3 million while cases rose by 21 per cent, reinforcing concerns about the continued prevalence of fraudulent investment opportunities, including those promoted through social media and online advertising. It also remains the scam type with one of the highest losses per case, over £16,000 compared with an average of £2,284 across all APP fraud types.

Advance fee scams recorded some of the most notable changes in the data for the first six months of the year, although the increase was starting to become evident in the latter part of 2025. Cases more than doubled compared with the first half of 2025 and losses increased by 73 per cent. The number of individual payments associated with these scams also increased compared to what we have seen in previous years.

This suggests not only more victims, but also evidence that victims are making multiple payments over longer periods before the fraud is identified. Industry intelligence indicates that some of this growth may be linked to emerging forms of high-value deposit scams and recruitment or employment-related fraud, trends that are increasingly being reported internationally.

What are advanced fee scams?

A common feature of advance fee fraud is that the victim is persuaded to make an upfront payment in expectation of receiving a larger benefit, asset, or opportunity that never materialises. For example:

- High-value goods scam: A victim is asked to pay a deposit or reservation fee to secure a high-value item, such as a car, boat, luxury watch, or construction equipment, which either does not exist or is never delivered.
- Employment or recruitment scam: A fraudster offers a job and requests upfront payments for training, equipment, security checks, visas, or administration fees before employment begins.
- Loan fee scam: A victim seeking credit is told they have been approved for a loan but must first pay an arrangement fee, insurance premium, or processing charge. The loan is never provided.

Purchase scams remain the largest APP fraud category by volume. Nearly 96,000 cases were recorded in the first half of 2026, accounting for around seven in ten APP fraud cases. While losses per case remain lower than in investment fraud, their scale and persistence means purchase scams continue to be a major source of consumer harm.

The continued growth in these channels indicate that fraudsters are becoming increasingly effective at identifying and exploiting behavioural vulnerabilities rather than technical weaknesses. Unlike traditional payment fraud, where security controls can often be deployed to block suspicious activity, malicious payee scams rely on techniques that create a false sense of trust, urgency or opportunity. The persistence of these scams, despite investment by firms in prevention, warnings and customer education, underlines the industrialised nature of modern fraud. The first half of 2026 provides further evidence that fraud is becoming less about stealing payment credentials and more about compromising trust.

Analysis of APP fraud enablers continues to demonstrate that the vast majority of scams originate outside the banking sector. Online platforms remain the single largest source of APP fraud, accounting for 58 per cent of cases in the first half of 2026. However, whilst online-enabled scams accounted for a somewhat lower 34 per cent of total losses in 2026 H1, this is the highest proportion since 2022. This suggests criminals are becoming increasingly effective at extracting larger losses from victims through online channels.

Telecommunications and messaging services remain the second most significant route used by fraudsters, accounting for 16 per cent of cases but 33 per cent of losses. While their share of overall volumes has remained broadly unchanged over recent years, these channels continue to be associated with higher-value scams, including impersonation and investment fraud.

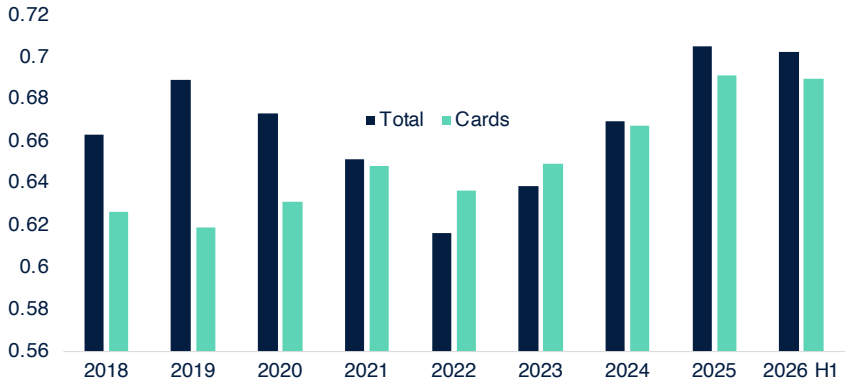
In the first half of 2026, the origin of 21 per cent of cases and 23 per cent of losses could not be ascertained. This reflects the increasingly complex and multi-channel nature of fraud, where criminals exploit a combination of online platforms, messaging services, telephone calls and other technologies throughout the lifecycle of a scam.

By contrast, total unauthorised fraud losses fell by two per cent to £343.5 million while cases declined by 17 per cent to 1.64 million. While this decline may offer some encouragement, it should be viewed alongside continued growth in APP fraud, and unauthorised fraud remains a sizeable component of the overall fraud picture. In the first half of this year, there were still just under 10,000 cases or £1.9 million in losses every day.

The improvement was driven primarily by card fraud, which remains the largest component of unauthorised fraud. Card fraud losses fell by four per cent to £286.4 million and cases declined by 17 per cent following the substantial increases recorded during 2024 and 2025. Remote purchase fraud, which has been the main driver of card fraud growth in recent years, recorded a ten per cent reduction in losses and a 19 per cent decline in cases.

The decline in card fraud is likely to reflect a combination of sustained industry investment in authentication, behavioural analytics and fraud detection systems, alongside changes in criminal behaviour. The industry also prevented £632 million of card fraud in the first six months of the year. Although this was lower than the figure reported in 2025, prevention levels remain historically elevated (chart 2), suggesting that security controls are making it increasingly difficult for criminals to monetise traditional card fraud at scale. Feedback from industry participants also suggests criminals are increasingly forced to undertake larger volumes of lower value attacks to generate returns, reducing profitability and increasing the likelihood of detection.

Chart 2. Unauthorised fraud prevention, percentage of fraud attempted



However, the reduction in unauthorised fraud should not be interpreted as evidence that the threat is diminishing. Rather, there are increasing signs that criminal activity is migrating towards social engineering-based attacks and fraud typologies which rely less on compromising systems and more on manipulating customer behaviour. This can include tactics which lead to a victim initiating a fraudulent payment by credit or debit card themselves – this is not captured in our APP data, which captures authorised payment frauds (bank transfer) only.

The rise in mobile banking losses seen in the first half of this year (and the latter part of 2025) may be a further example of this migration. UK Finance's UK Payment Markets report has shown strong growth in users of mobile banking channels in recent years, and with greater usage we are likely to see a corresponding increase in fraud via these channels. Whilst the rise in mobile banking users has outpaced the increase in fraud cases until this year, 2026 H1 saw an 18 per cent increase in mobile banking fraud losses and a 61 per cent increase in cases. Again, the compromise of personal information may be contributing to this rise.

The escalating use of social engineering reflects a broader pattern seen repeatedly over the past decade: as successful interventions close down one route to fraud, criminals seek alternative pathways.

The data also highlights the need for payment service providers to prepare for the unexpected. Several smaller fraud categories recorded large increases during the first half of the year. Unauthorised telephone banking losses increased by 57 per cent and cases more than doubled, while CEO fraud losses and cases more than doubled. Impersonation fraud involving police or bank staff also increased after a prolonged period of decline. Although these frauds remain relatively small when measured against overall losses, they demonstrate how quickly criminal groups can identify and exploit weaknesses in customer behaviour, operational processes or emerging technologies.

In many cases this is less about entirely new forms of fraud and more about the reinvention of familiar tactics. Criminals are increasingly able to enhance traditional fraud methodologies using richer personal data, automated communications, artificial intelligence tools and more sophisticated social engineering techniques. While industry feedback suggests these emerging threats can often be identified and disrupted quickly, they can nevertheless generate harm before effective countermeasures are deployed.

Taken together, the first half of 2026 presents a mixed picture. Significant progress continues to be made in preventing many forms of unauthorised fraud, demonstrating the value of sustained investment in security and detection capabilities. At the same time, the sharp increase in APP fraud highlights the growing challenge posed by scams that are frequently initiated outside the financial sector and rely on the manipulation of individuals rather than the compromise of payment systems.

These developments reinforce the importance of maintaining a balanced view across the fraud landscape, not just focusing solely on the largest categories, and ensuring responses remain flexible as criminal methodologies evolve. The latest figures reinforce the central lesson from recent years: fraud is highly adaptive. Continued progress will depend on strong industry investment, effective information sharing and a coordinated cross-sector response involving payments providers, technology companies, telecommunications firms, regulators and law enforcement.

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) 2026 vs H1 (Jan to June) 2025 unless otherwise stated.

Fraud in the first half of 2026

£659.5M

stolen through fraud in the first half of 2025

1.8M

confirmed cases, 14 per cent less than in 2025

£810.5M

of unauthorised fraud prevented by industry, equivalent to 70p in every £1 attempted.

Unauthorised fraud

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

Authorised fraud

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

Losses

The total value of gross losses (unauthorised and authorised)

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Unauthorised	£397.3m	£333.0m	£352.4m	£374.5m	£341.2m	£367.6m	£366.8m	£377.4m	£350.7m	£352.7m	£343.5m	**-2%**
Authorised	£301.5m	£281.8m	£241.9m	£243.3m	£239.3m	£220.4m	£229.8m	£254.2m	£258.2m	£318.2m	£316.0m	**22%**
Total	£698.8m	£614.8m	£594.3m	£617.8m	£580.5m	£587.9m	£596.6m	£631.6m	£608.9m	£670.9m	£659.5m	**8%**

Cases

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

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Unauthorised	1,496,840	1,415,627	1,397,765	1,383,546	1,264,275	1,465,532	1,653,770	1,790,711	1,961,645	1,852,487	1,637,455	**-17%**
Authorised	101,540	94,456	95,167	112,205	116,316	116,111	120,184	111,290	110,822	137,248	138,345	**25%**
Total	1,598,380	1,510,083	1,492,932	1,495,751	1,380,591	1,581,643	1,773,954	1,902,001	2,072,467	1,989,735	1,775,800	**-14%**

Total unauthorised fraud

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

Unauthorised fraud losses were **£343.5 million** in the first six months of 2026, a decrease of two per cent from the same period in 2025.

There were **1.64 million** confirmed cases of unauthorised fraud reported in H1 2026, a 17 per cent decrease on the total reported in H1 2025.

The industry prevented a further **£810.5 million** of unauthorised fraud – equivalent to 70p in every £1 of attempted unauthorised fraud being stopped without a loss occurring.

Cards

Prevented: **£632.2m** (-7%)
Losses: **£286.4m** (-4%)
Cases: **1.62m** (-17%)

Cheques

Prevented: **£27.3m** (-50%)
Losses: **£0.9m** (-59%)
Case: **328** (-2%)

Remote Banking

Prevented: **£151.0m** (+24%)
Losses: **£56.2m** (+15%)
Case: **21,905** (+38%)

Total unauthorised card fraud

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H2 2026	Change
Prevented	£481.7m	£484.9m	£492.0m	£482.2m	£519.5m	£502.2m	£566.9m	£623.6m	£683.3m	£650.0m	£632.2m	-7%
Cases	1,444,996	1,378,206	1,371,469	1,361,403	1,245,224	1,445,974	1,635,774	1,773,813	1,945,384	1,830,307	1,615,222	-17%
Gross Loss	£261.3m	£263.2m	£270.2m	£286.0m	£260.0m	£291.4m	£286.3m	£306.2m	£299.8m	£295.1m	£286.4m	-4%

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 £286.4 million in the first half of 2026, a decrease of four per cent on the same period in 2025.

Over this period the overall value of card spending by UK cardholders increased slightly. Card fraud as a proportion of card purchases has fallen from 6.9p in the first half of 2025 to 6.6p in the first half of 2026. A total of £632.2 million of card fraud was stopped by banks and card companies in the first six months of 2026. This is equivalent to £6.88 in every £10 of attempted card fraud prevented without a loss occurring.

Remote Purchase (Card Not Present)

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Cases	1,264,562	1,159,264	1,136,886	1,084,140	984,059	1,143,142	1,360,004	1,470,289	1,660,003	1,536,959	1,351,449	-19%
Gross Loss	£210.1m	£202.4m	£198.1m	£197.6m	£174.5m	£186.0m	£200.8m	£211.7m	£216.4m	£207.1m	£195.4m	-10%

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 decreased by ten per cent to £195.4 million in the first six months of 2026. The number of cases decreased by 19 per cent to 1.35 million.

Feedback suggests that whilst there has been a decrease in this type of fraud in the first six months of 2026, criminals continue to adopt 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. The decrease is also likely to be a consequence of criminals tricking customers into making card transactions themselves which is classified as an authorised card fraud and is therefore not included in these numbers.

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 £174.5 million in the first half of 2026, an increase of nine per cent when compared with the same period in 2025.

Lost and Stolen

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Cases	144,713	180,788	185,609	215,731	188,409	209,140	209,680	231,902	220,608	228,584	206,015	-7%
Gross Loss	£35.1m	£42.1m	£46.9m	£53.2m	£48.6m	£55.4m	£51.7m	£59.9m	£52.0m	£57.8m	£57.3m	10%

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 ten per cent in H1 2026 and totalled £57.3 million. The number of incidents reported decreased seven per cent to just over 206,000 cases.

Card Not Received

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Cases	4,126	4,815	5,093	3,755	2,874	3,059	3,541	3,857	3,950	3,939	3,266	-17%
Gross Loss	£2.0m	£2.0m	£1.9m	£2.0m	£1.4m	£1.6m	£1.9m	£1.0m	£1.3m	£1.5m	£1.5m	14%

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

Card not received fraud losses increased by 14 per cent to £1.5 million during January to June 2026, case volumes decreased by 17% 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 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Cases	14,640	10,268	9,664	9,930	8,633	9,437	7,610	7,378	8,541	9,936	10,382	22%
Gross Loss	£2.6m	£2.1m	£2.2m	£2.5m	£2.3m	£2.4m	£2.1m	£1.8m	£2.3m	£2.5m	£2.5m	9%

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

Counterfeit card losses totalled £2.5 million in H1 2026, a rise of nine per cent on the total reported in 2025. Case volumes rose by 22 per cent to 10,382.

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.

Card ID Theft

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Cases	16,955	23,071	34,217	47,847	61,249	81,196	54,939	60,387	52,282	50,889	44,110	**-16%**
Gross Loss	£11.5m	£14.7m	£21.1m	£30.6m	£33.1m	£46.0m	£29.8m	£31.7m	£27.7m	£26.3m	£29.6m	**7%**

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 increased seven per cent in the first six months of 2026 compared with the same period in 2025, rising to £29.6 million. The number of individual cases decreased over the same period, dropping by 16% to 44,110 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 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
UK Retail	£19.6m	£27.3m	£33.3m	£38.8m	£38.4m	£50.3m	£38.0m	£47.3m	£40.4m	£45.6m	£44.8m	11%

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 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
UK ECOM	£121.9m	£114.2m	£111.3m	£109.2m	£97.4m	£105.0m	£112.7m	£118.2m	£122.6m	£123.4m	£120.7m	-2%

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 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
UK ATM	£12.0m	£12.4m	£12.9m	£13.2m	£12.7m	£12.9m	£12.8m	£13.0m	£12.9m	£12.8m	£12.9m	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 2026. Most of this fraud is thought to be perpetuated through distraction thefts and card entrapment at ATMs.

UK / International Card Fraud

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
UK	£187.6m	£196.4m	£202.4m	£213.8m	£197.2m	£219.7m	£205.8m	£223.6m	£223.7m	£221.5m	£211.8m	-5%
INT	£73.7m	£66.8m	£67.9m	£72.2m	£62.8m	£71.7m	£80.5m	£82.6m	£76.1m	£73.6m	£74.6m	-2%

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 decreased by five per cent to £211.8 million and international fraud losses by two per cent, to £74.6 million.

Unauthorised Cheque Fraud

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Prevented	£21.0m	£12.0m	£10.5m	£9.3m	£7.3m	£5.0m	£11.9m	£41.8m	£54.7m	£52.7m	£27.3m	**-50%**
Cases	382	433	415	551	559	638	636	470	336	459	328	**-2%**
Gross Loss	£3.5m	£2.9m	£3.2m	£4.3m	£2.9m	£2.8m	£3.8m	£4.3m	£2.2m	£1.9m	£0.9m	**-59%**

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 59 per cent in the first half of 2026, while the number of cases fell two per cent to 328 cases. Both figures are the lowest ever reported for a six month period in the category.

Unauthorised Remote Banking

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Prevented	£230.3m	£135.3m	£88.1m	£86.0m	£104.6m	£113.5m	£149.3m	£116.2m	£121.9m	£118.3m	£151.0m	**24%**
Cases	51,462	36,988	25,881	21,592	18,492	18,920	17,360	16,428	15,925	21,721	21,905	**38%**
Gross Loss	£132.5m	£67.0m	£78.9m	£84.2m	£78.3m	£73.4m	£76.7m	£66.8m	£48.8m	£55.6m	£56.2m	**15%**

Remote banking fraud losses are organised into three categories: internet, telephone and mobile banking. It occurs when a criminal gains unauthorised access to a customers' account(s). They use a range of techniques, including phishing, smishing, vishing, malware infections, remote access scams, credential theft, data breaches, account takeover attacks, SIM-swap fraud and other forms of social engineering. These methods enable criminals to compromise customer credentials, bypass authentication controls, or take control of customer devices in order to conduct unauthorised transactions.

Total remote banking fraud amounted to £56.2 million in the first half of 2026, a 15 per cent increase compared to the amount lost in the first six months 2025. The number of cases of remote banking fraud increased by 38 per cent to 21,905.

UK Finance research shows that last year, 91 per cent of the adult population used at least one form of remote banking.

A total of £151 million of attempted remote banking fraud was stopped by bank security systems in the first six months of 2026. This is equivalent to 73p in every £1 of fraud attempted being prevented.

In addition, 11 per cent (£6.4 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 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Cases	42,628	29,929	18,001	14,035	7,775	5,894	4,744	4,432	4,756	4,806	3,353	**-29%**
Gross Loss	£108.0m	£50.3m	£55.5m	£58.6m	£50.5m	£38.2m	£44.2m	£33.6m	£24.0m	£28.7m	£25.4m	**6%**

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 increased during H1 2026, rising six per cent to £25.4 million when compared with the same period in 2025. Case volumes decreased, falling 29 per cent to 3,353 cases.

Unauthorised Telephone Banking

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Cases	2,545	2,078	1,776	1,300	1,533	2,178	1,723	2,010	1,315	1,589	2,679	**104%**
Gross Loss	£7.5m	£8.0m	£7.4m	£7.3m	£7.3m	£10.3m	£8.8m	£7.9m	£3.7m	£4.2m	£5.8m	**57%**

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.

Typically, criminals employ a range of social engineering techniques to trick victims into giving away their personal and financial information. This includes using impersonation scam calls, emails or text messages typically exploiting current affairs by impersonating trusted organisations.

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 57 per cent to £5.8 million in the first six months of 2026.

During the same period the number of telephone banking cases rose by 104% to 2,679, however, telephone banking only accounts for less than 0.2% of all confirmed unauthorised fraud cases.

Unauthorised Mobile Banking

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Cases	6,289	4,981	6,104	6,257	9,184	10,848	10,893	9,986	9,854	15,326	15,873	**61%**
Gross Loss	£17.1m	£8.7m	£16.0m	£18.2m	£20.6m	£24.9m	£23.7m	£25.3m	£21.1m	£22.7m	£25.0m	**18%**

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.

Typically, criminals employ a range of social engineering techniques to trick victims into giving away their personal and financial information. This includes using impersonation scam calls, emails or text messages typically exploiting current affairs by impersonating trusted organisations."

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 18 per cent to £25.0 million in the first six months of 2026, 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 61 per cent to 15,873; another record high for the first half of the year.

Authorised Push Payment (APP)

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Cases	101,540	94,456	95,167	112,205	116,316	116,111	120,184	111,290	110,822	137,248	138,345	**25%**
Payments	172,622	172,515	166,327	205,939	211,560	205,900	217,238	210,941	226,551	292,882	293,285	**29%**
Gross Loss	£301.5m	£281.8m	£241.9m	£243.3m	£239.3m	£220.4m	£229.8m	£254.2m	£258.2m	£318.2m	£316.0m	**22%**
Returned to Victim	£125.8m	£131.9m	£135.6m	£150.0m	£152.8m	£134.5m	£128.5m	£143.2m	£159.6m	£194.7m	£205.7m	**29%**

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:

- 58% of fraud cases are enabled by online sources. These cases tend to include lower-value scams such as purchase fraud and therefore account for 34% 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 33% 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.

	2022		2023		2024		2025		H1 2026	
	Volume	Value	Volume	Value	Volume	Value	Volume	Value	Volume	Value
Online	78%	36%	76%	30%	70%	29%	66%	30%	58%	33%
Telecommunications	18%	45%	16%	43%	16%	36%	17%	29%	16%	33%
Email	2%	12%	1%	11%	1%	10%	1%	9%	1%	5%
Other	1%	3%	2%	5%	3%	7%	5%	8%	4%	6%
Unknown	1%	4%	5%	11%	10%	18%	11%	24%	21%	23%

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 Contingent Reimbursement (CRM) voluntary code.

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

UK Finance reimbursement reporting	In scope mandatory reimbursement
Payments from personal accounts and businesses of all sizes	Payments made from personal, micro-businesses and charity accounts
Payments authorised in the UK and received both in the UK and internationally	Only payments authorised in the UK and received in a UK account
Payments of any value	Payments up to a maximum 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 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Cases	50,327	49,406	53,907	63,263	76,943	79,573	86,087	80,711	80,187	95,622	95,830	**20%**
Payments	64,948	67,463	72,282	86,836	107,655	111,939	122,529	117,262	118,207	144,669	148,676	**26%**
Loss	£32.3m	£31.8m	£31.1m	£35.9m	£40.9m	£45.1m	£48.1m	£50.6m	£53.2m	£64.9m	£66.0m	**24%**
Returned to Victim	£9.3m	£11.7m	£16.5m	£21.6m	£25.7m	£30.1m	£28.8m	£31.9m	£39.8m	£52.0m	£53.7m	**35%**

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 95,830 confirmed cases accounting for 69 per cent of the total number of all APP scam cases reported in the first half of 2026. A total of £66.0 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 £53.7 million (81%) of the losses to the victims.

Investment Scam

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Cases	6,224	5,850	5,161	4,924	5,112	5,114	5,660	6,149	6,476	8,417	7,805	**21%**
Payments	17,567	18,098	14,928	15,583	16,942	16,454	19,072	22,514	25,209	32,004	29,191	**16%**
Loss	£90.6m	£81.1m	£58.4m	£55.7m	£57.2m	£50.7m	£63.0m	£95.1m	£97.8m	£123.6m	£126.3m	**29%**
Returned to Victim	£34.8m	£37.0m	£29.4m	£29.2m	£33.5m	£25.5m	£30.5m	£42.8m	£47.2m	£59.3m	£68.1m	**44%**

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 29 per cent in January to June 2026 to £126.3million. Investment scams continued to account for the largest value of all eight APP scam types accounting for 40 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 would have occurred some time ago.

Payment service providers returned £68.1 million (54 per cent) of the losses to the victims.

Romance Scam

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Cases	1,479	1,791	1,644	2,005	2,120	2,040	2,527	2,683	2,995	3,340	3,800	**27%**
Payments	11,489	14,325	13,199	17,021	18,889	20,689	23,392	25,884	27,792	33,709	35,109	**26%**
Loss	£12.7m	£18.2m	£14.6m	£16.7m	£18.5m	£18.1m	£15.2m	£16.6m	£20.5m	£18.6m	£16.8m	**-18%**
Returned to Victim	£4.3m	£7.8m	£7.2m	£9.3m	£11.6m	£11.2m	£9.6m	£10.2m	£12.6m	£13.6m	£11.6m	**-8%**

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 £16.8 million was lost to romance scams during January to June 2026, a decrease of 18 per cent when compared with the same period in 2025. 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 £11.6 million to victims or 69 per cent of the total.

Advance Fee Scam

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Cases	9,064	11,431	11,472	15,857	12,238	11,610	9,933	7,527	7,572	16,508	16,481	118%
Payments	16,233	20,737	20,609	30,622	27,047	23,912	21,669	19,085	27,664	55,597	51,229	85%
Loss	£14.1m	£18.1m	£14.2m	£18.0m	£15.1m	£16.3m	£17.1m	£18.2m	£19.6m	£38.8m	£34.0m	73%
Returned to Victim	£5.3m	£6.1m	£6.3m	£11.5m	£9.6m	£11.7m	£10.6m	£9.7m	£13.1m	£21.8m	£24.0m	83%

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.

There has also been an increased number of recruitment scams reported in more recent times, these scams involve criminals advertising fictitious jobs or career opportunities, usually on social media platforms with the aim of scamming victims into paying money upfront or compromising vast amounts of personal information.

Advance fee scams were the second most common form of APP scam in the first half of 2026, accounting for twelve per cent of the total number of cases.

A total of £34.0 million was lost to advance fee scams, an increase of 73 percent compared with the first six months of 2025. Payment service providers returned £24.0 million (71 per cent) of the losses to the victims.

Invoice and Mandate Scam

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Cases	2,053	2,277	1,591	1,749	1,665	1,445	1,168	1,193	1,176	1,129	1,041	-11%
Payments	2,813	3,354	2,340	2,625	2,352	2,060	1,649	1,749	1,921	1,808	1,457	-24%
Loss	£27.1m	£29.6m	£25.5m	£24.0m	£24.8m	£25.4m	£26.0m	£17.1m	£20.3m	£20.9m	£18.7m	-8%
Returned to Victim	£10.8m	£11.7m	£13.6m	£12.8m	£12.2m	£11.4m	£11.9m	£9.2m	£9.5m	£10.4m	£7.0m	-26%

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

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

Invoice and mandate scam losses totalled £18.7 million in the first half of 2026, a decrease of eight per cent when compared with the same period in 2025. 75 per cent (£14.0 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 £7.0 million (38 per cent) of the losses to the victims.

CEO Scam

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Cases	230	231	200	232	196	215	157	120	78	119	171	**119%**
Payments	331	347	297	318	302	289	287	165	106	146	298	**181%**
Loss	£6.1m	£6.6m	£7.9m	£5.6m	£6.9m	£4.7m	£7.8m	£4.1m	£1.6m	£4.0m	£3.3m	**107%**
Returned to Victim	£1.6m	£1.2m	£2.2m	£1.4m	£1.4m	£1.7m	£1.3m	£1.0m	£0.4m	£0.8m	£0.8m	**121%**

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 2026, accounting for less than one per cent of total cases. A total of £3.3 million was lost. CEO scam has the highest average case value of all eight scam types with an average of just under £20,000 being lost per confirmed case.

Payment service providers returned £0.8 million (24 per cent) of the losses to victims in the first six months of 2026.

Impersonation: Police/Bank Staff

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Cases	17,521	11,885	9,138	7,810	5,976	4,618	4,383	3,406	3,162	2,854	4,073	**29%**
Payments	34,774	28,032	22,533	25,997	17,910	12,842	11,834	8,997	10,213	8,983	10,320	**1%**
Loss	£75.6m	£61.8m	£59.4m	£50.4m	£43.5m	£35.4m	£33.2m	£34.6m	£27.1m	£28.4m	£31.1m	**15%**
Returned to Victim	£40.6m	£38.6m	£42.0m	£40.4m	£35.0m	£26.4m	£22.3m	£25.0m	£22.3m	£21.8m	£25.6m	**15%**

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 10 per cent of all APP scam losses in H1 2026 totalling £31.1 million.

Prevention methods such as effective warning messages during the payment journey will also have helped contribute to combatting this type of fraud. Payment service providers were able to return £25.6 million (82 per cent) of the losses to victims.

Impersonation: Other

	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Cases	14,642	11,585	12,054	16,365	12,066	11,496	10,269	9,501	9,176	9,259	9,144	**0%**
Payments	24,467	20,159	20,139	26,937	20,463	17,715	16,806	15,285	15,439	15,966	17,005	**10%**
Loss	£43.0m	£34.6m	£30.8m	£37.0m	£32.6m	£24.7m	£19.3m	£17.9m	£18.0m	£18.9m	£19.8m	**10%**
Returned to Victim	£19.2m	£17.7m	£18.5m	£23.8m	£23.9m	£16.5m	£13.5m	£13.5m	£14.8m	£14.9m	£14.8m	**1%**

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 £19.8 million was lost to this type of scam during the first six months of 2026, an increase of ten per cent when compared with 2025.

Payment service providers were able to return £14.8 million of the losses to customers or 75 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 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Faster Payment	£263.7m	£240.8m	£208.3m	£212.8m	£199.1m	£181.1m	£175.8m	£208.5m	£209.6m	£251.3m	£252.2m	20%
CHAPS	£9.3m	£13.2m	£8.8m	£5.1m	£13.1m	£10.0m	£11.6m	£4.3m	£6.1m	£11.4m	£11.2m	83%
BACS	£11.1m	£9.3m	£12.5m	£11.4m	£13.2m	£14.6m	£20.2m	£7.0m	£8.4m	£10.7m	£8.4m	0%
Intra Bank Transfer ("on us")	£5.3m	£2.3m	£0.5m	£1.1m	£1.6m	£1.0m	£3.2m	£3.5m	£4.2m	£4.9m	£4.9m	17%
International	£12.2m	£16.2m	£11.8m	£12.9m	£12.3m	£13.6m	£19.0m	£30.9m	£29.8m	£39.9m	£39.2m	32%
Total	£301.5m	£281.8m	£241.9m	£243.3m	£239.3m	£220.4m	£229.8m	£254.2m	£258.2m	£318.2m	£316.0m	22%

Payment Type Volumes	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Faster Payment	167,720	167,731	163,142	201,822	207,959	201,574	211,867	203,011	213,769	272,281	273,648	28%
CHAPS	435	329	398	152	196	253	144	172	78	105	120	54%
BACS	729	966	911	1,316	1,284	1,246	1,073	1,061	1,333	1,596	1,276	-4%
Intra Bank Transfer ("on us")	2,100	1,258	532	710	812	834	1,872	2,996	6,421	11,538	9,898	54%
International	1,638	2,231	1,344	1,939	1,309	1,993	2,282	3,701	4,950	7,362	8,343	69%
Total	172,622	172,515	166,327	205,939	211,560	205,900	217,238	210,941	226,551	292,882	293,285	29%

APP: Payment Channel

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

Payment Channel Values	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Branch	£27.2m	£29.3m	£25.0m	£20.7m	£27.5m	£22.5m	£22.9m	£17.2m	£18.3m	£17.5m	£18.8m	3%
Internet Banking	£171.4m	£157.7m	£135.6m	£139.0m	£129.5m	£95.4m	£96.1m	£91.0m	£105.4m	£113.1m	£112.2m	6%
Telephone Banking	£11.3m	£13.1m	£8.7m	£6.9m	£7.7m	£11.2m	£8.7m	£12.1m	£7.4m	£12.9m	£7.5m	1%
Mobile Banking	£91.5m	£81.7m	£72.5m	£76.8m	£74.7m	£91.2m	£102.0m	£133.9m	£127.0m	£174.7m	£177.5m	40%
Total	£301.5m	£281.8m	£241.9m	£243.3m	£239.3m	£220.4m	£229.8m	£254.2m	£258.2m	£318.2m	£316.0m	22%

Payment Channel Volumes	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Branch	4,070	4,181	3,754	4,811	4,480	3,695	2,820	2,754	2,943	2,346	2,370	-19%
Internet Banking	62,789	67,227	63,229	75,471	72,370	51,087	40,237	40,024	46,263	53,820	53,037	15%
Telephone Banking	2,725	3,524	3,203	2,973	3,710	2,908	1,549	1,635	1,744	1,900	1,441	-17%
Mobile Banking	103,038	97,583	96,141	122,668	131,000	148,209	172,632	166,528	175,601	234,816	236,437	35%
Total	172,622	172,515	166,327	205,923	211,560	205,899	217,238	210,941	226,551	292,882	293,285	29%

Our Fraud Data

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

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

Some caveats are required for the tables in the document.

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

Methodology for Data Collection

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

Validation check

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

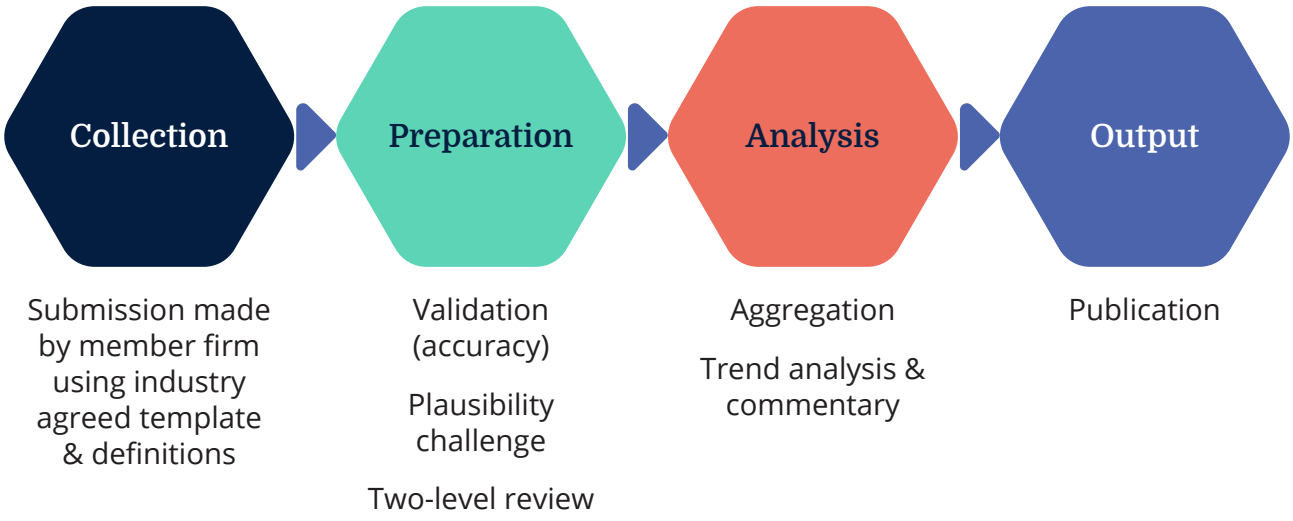
Data plausibility - inputs

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

Data plausibility – outputs

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

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



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

Appendix

Cases

Type	Category	Sub Category	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Unauthorised	**Card**	**Lost & stolen**	144,713	180,788	185,609	215,731	188,409	209,140	209,680	231,902	220,608	228,584	206,015	**-7%**
Unauthorised	**Card**	**CNR**	4,126	4,815	5,093	3,755	2,874	3,059	3,541	3,857	3,950	3,939	3,266	**-17%**
Unauthorised	**Card**	**Counterfeit**	14,640	10,268	9,664	9,930	8,633	9,437	7,610	7,378	8,541	9,936	10,382	**22%**
Unauthorised	**Card**	**Remote purchase**	1,264,562	1,159,264	1,136,886	1,084,140	984,059	1,143,142	1,360,004	1,470,289	1,660,003	1,536,959	1,351,449	**-19%**
Unauthorised	**Card**	**Card ID Theft**	16,955	23,071	34,217	47,847	61,249	81,196	54,939	60,387	52,282	50,889	44,110	**-16%**
Unauthorised	**Cheque**	**Cheque**	382	433	415	551	559	638	636	470	336	459	328	**-2%**
Unauthorised	**Remote Banking**	**Internet Banking**	42,628	29,929	18,001	14,035	7,775	5,894	4,744	4,432	4,756	4,806	3,353	**-29%**
Unauthorised	**Remote Banking**	**Telephone Banking**	2,545	2,078	1,776	1,300	1,533	2,178	1,723	2,010	1,315	1,589	2,679	**104%**
Unauthorised	**Remote Banking**	**Mobile Banking**	6,289	4,981	6,104	6,257	9,184	10,848	10,893	9,986	9,854	15,326	15,873	**61%**
Authorised	**Payment**	**Invoice & Mandate**	2,053	2,277	1,591	1,749	1,665	1,445	1,168	1,193	1,176	1,129	1,041	**-11%**
Authorised	**Payment**	**CEO**	230	231	200	232	196	215	157	120	78	119	171	**119%**
Authorised	**Payment**	**IMP: Police/Bank**	17,521	11,885	9,138	7,810	5,976	4,618	4,383	3,406	3,162	2,854	4,073	**29%**
Authorised	**Payment**	**IMP: Other**	14,642	11,585	12,054	16,365	12,066	11,496	10,269	9,501	9,176	9,259	9,144	**0%**
Authorised	**Payment**	**Purchase**	50,327	49,406	53,907	63,263	76,943	79,573	86,087	80,711	80,187	95,622	95,830	**20%**
Authorised	**Payment**	**Investment**	6,224	5,850	5,161	4,924	5,112	5,114	5,660	6,149	6,476	8,417	7,805	**21%**
Authorised	**Payment**	**Romance**	1,479	1,791	1,644	2,005	2,120	2,040	2,527	2,683	2,995	3,340	3,800	**27%**
Authorised	**Payment**	**Advance Fee**	9,064	11,431	11,472	15,857	12,238	11,610	9,933	7,527	7,572	16,508	16,481	**118%**

Losses

Type	Category	Sub Category	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	H2 2023	H1 2024	H2 2024	H1 2025	H2 2025	H1 2026	Change
Unauthorised	Card	Lost & stolen	£35.1m	£42.1m	£46.9m	£53.2m	£48.6m	£55.4m	£51.7m	£59.9m	£52.0m	£57.8m	£57.3m	**10%**
Unauthorised	Card	CNR	£2.0m	£2.0m	£1.9m	£2.0m	£1.4m	£1.6m	£1.9m	£1.0m	£1.3m	£1.5m	£1.5m	**14%**
Unauthorised	Card	Counterfeit	£2.6m	£2.1m	£2.2m	£2.5m	£2.3m	£2.4m	£2.1m	£1.8m	£2.3m	£2.5m	£2.5m	**9%**
Unauthorised	Card	Remote purchase	£210.1m	£202.4m	£198.1m	£197.6m	£174.5m	£186.0m	£200.8m	£211.7m	£216.4m	£207.1m	£195.4m	**-10%**
Unauthorised	Card	Card ID Theft	£11.5m	£14.7m	£21.1m	£30.6m	£33.1m	£46.0m	£29.8m	£31.7m	£27.7m	£26.3m	£29.6m	**7%**
Unauthorised	Cheque	Cheque	£3.5m	£2.9m	£3.2m	£4.3m	£2.9m	£2.8m	£3.8m	£4.3m	£2.2m	£1.9m	£0.9m	**-59%**
Unauthorised	Remote Banking	Internet Banking	£108.0m	£50.3m	£55.5m	£58.6m	£50.5m	£38.2m	£44.2m	£33.6m	£24.0m	£28.7m	£25.4m	**6%**
Unauthorised	Remote Banking	Telephone Banking	£7.5m	£8.0m	£7.4m	£7.3m	£7.3m	£10.3m	£8.8m	£7.9m	£3.7m	£4.2m	£5.8m	**57%**
Unauthorised	Remote Banking	Mobile Banking	£17.1m	£8.7m	£16.0m	£18.2m	£20.6m	£24.9m	£23.7m	£25.3m	£21.1m	£22.7m	£25.0m	**18%**
Authorised	Payment	Invoice & Mandate	£27.1m	£29.6m	£25.5m	£24.0m	£24.8m	£25.4m	£26.0m	£17.1m	£20.3m	£20.9m	£18.7m	**-8%**
Authorised	Payment	CEO	£6.1m	£6.6m	£7.9m	£5.6m	£6.9m	£4.7m	£7.8m	£4.1m	£1.6m	£4.0m	£3.3m	**107%**
Authorised	Payment	IMP: Police/Bank	£75.6m	£61.8m	£59.4m	£50.4m	£43.5m	£35.4m	£33.2m	£34.6m	£27.1m	£28.4m	£31.1m	**15%**
Authorised	Payment	IMP: Other	£43.0m	£34.6m	£30.8m	£37.0m	£32.6m	£24.7m	£19.3m	£17.9m	£18.0m	£18.9m	£19.8m	**10%**
Authorised	Payment	Purchase	£32.3m	£31.8m	£31.1m	£35.9m	£40.9m	£45.1m	£48.1m	£50.6m	£53.2m	£64.9m	£66.0m	**24%**
Authorised	Payment	Investment	£90.6m	£81.1m	£58.4m	£55.7m	£57.2m	£50.7m	£63.0m	£95.1m	£97.8m	£123.6m	£126.3m	**29%**
Authorised	Payment	Romance	£12.7m	£18.2m	£14.6m	£16.7m	£18.5m	£18.1m	£15.2m	£16.6m	£20.5m	£18.6m	£16.8m	**-18%**
Authorised	Payment	Advance Fee	£14.1m	£18.1m	£14.2m	£18.0m	£15.1m	£16.3m	£17.1m	£18.2m	£19.6m	£38.8m	£34.0m	**73%**

Contributing Members

List of members who have contributed data to this publication

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

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

© 2026, UK Finance