UK FINANCE

2023 HALF YEAR FRAUD UPDATE

In association with:

feedzai

ukfinance.org.uk

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.
- All percentage changes relate to H1 (Jan to June) 2023 vs H1 (Jan to June) 2022 unless otherwise stated.

FOREWORD

The latest UK Finance figures show that fraud continues to be one of the most prevalent crimes in the UK. From impersonating companies and creating fake investment adverts, to stealing card details and taking over personal accounts, criminals are using social engineering to ruthlessly target their victims. In the first six months of this year alone, criminals stole over half a billion pounds.

Fraud on this scale not only impacts consumers, it also increases the costs of conducting business, damages the reputation of the UK and threatens our economy.

The financial sector is at the forefront of the fightback. Our investment and commitment to tackling fraud has contributed to a reduction in losses compared to last year, with advanced security systems helping to prevent £655 million from being stolen. However, the overall picture is still not a positive one and much more needs to be done.

The real cost of fraud

This isn't just about money. Many types of fraud, particularly romance and investment scams, involve severe psychological manipulation of the victim. Regardless of the amount of money involved, these callous crimes can cause psychological harm and lead to people losing their confidence, their trust, and their sense of security.

This is one of the key reasons why the financial services industry, works so tirelessly and invests so much in trying to reduce the number of victims of fraud.

Protecting customers

For example, where criminals have been impersonating financial services firms, banks have introduced new warning messages during the payment journey – leading to a 35 per cent reduction in this kind of fraud.

UK Finance continues to invest in public education as well, through our Take Five to Stop Fraud campaign and our anti-money muling campaign Don't Be Fooled, which is helping educate school children and young adults to the risks.

The financial services sector also refunds victims, which is vitally important and our figures this year show an increase in reimbursement.

Refunding stolen money does not stop the crime or prevent the emotional or psychological damage, and it risks incentivising the criminal. We need a balanced approach that helps to protect, educate and empower consumers, and looks more closely at where fraud originates.

What needs to happen

Our report shows that 77 per cent of all Authorised Push Payment (APP) fraud in the first half of 2023 originated online platform, through fake websites, social media posts and more. In terms of the value of losses, 45 per cent began through telecommunications like scam phone calls and texts.

The fact that currently these sectors bear no responsibility for reimbursing victims means that there is little commercial incentive for them to truly tackle the problem that proliferates on their sites, platforms and networks. This needs to change. If we are to see a real difference, we need them to do more with us to protect consumers and share the burden of the fight against criminals.

There are already important moves from the government on this, including the Online Safety Bill and Online Advertising Programme, as well as the new fraud strategy which appointed Anthony Browne as the cross-sector anti-fraud champion. We hope collectively these moves result in shared responsibilities, effective regulation and cross-sector action.

Prosecution also plays a crucial part in preventing fraud and the financial sector and law enforcement work closely together on this. The Dedicated Card and Payment Crime Unit (DCPCU) is a collaboration between UK Finance, the City of London Police and the Metropolitan Police Service. This specialist unit prevented losses of just over £22 million in the first six months of 2023 alone.

There is also the Banking Protocol, which enables bank branch staff to call 999 and receive an emergency response when they believe a customer may be the victim of a scam. It has prevented a significant amount of fraud and has led to almost 1300 arrests.

The government's new fraud strategy also makes fraud a strategic policing requirement and creates a new fraud focused team within the intelligence community. But there still needs to be greater investment to ensure law enforcement and government departments can tackle the scale of fraud we face today.

Finally, the sharing of data and intelligence is critical to the fight against fraud. Improving how this is done more broadly, and understanding where to collectively prioritise to make the most impact would help. We look forward to continuing to work with the public sector on a new Data Strategy under the Economic Crime Plan.

Conclusion

Criminals will continue to try to ruthlessly exploit the trust of people across the UK, including the most vulnerable. Fraud is an ever evolving and complex threat to people and businesses and technological change and the greater prevalence of AI will continue to make it more challenging. It is only through collective action across government, law enforcement and all industries involved that we can truly stop fraud and protect people from all the harm it causes.

Ben Donaldson,
Managing Director, Economic Crime,
UK Finance

DRIVERS BEHIND THE FIGURES:

The latest figures released by UK Finance highlight that fraud fell in the first six months of 2023 with a total of £580 million being stolen by criminals. This is a decrease of two per cent compared with the same period in 2022. The advanced security systems used by banks also prevented £651 million from being stolen.

In today's world of fraud and scams, criminals mainly focus on social engineering their victims. These tactics include scam phone calls, text messages and emails, as well as fake websites and social media posts. Their aim is to trick people into handing over personal details and passwords. This information is then used to target victims and convince them to either authorise payments that they are unaware of or encourage them to make the payment themselves.

Typically, criminals first focus their attempts on socially engineering personal information from their victims with a view to committing Authorised Push Payment (APP) fraud in which the victim makes the payment themselves. If this is not successful, the criminal often has enough personal information to enable them instead to impersonate their victims, with a view to either taking control of their existing accounts or applying for credit cards in their name. The fraud types that have seen an increase in losses are those that require the theft of significant amounts of personal information, such as card ID theft.

APP fraud has fallen in the first half of 2023 (down one per cent to £239.3 million) yet is still 27 per cent higher than the total reported for the same period in 2020. Confirmed case volumes totalled over 116,000 (up 22 per cent compared with H1 2022) and this therefore remains a focus for the financial services sector.

The main driver behind the increase in confirmed cases is purchase scams which continued to rise, totalling just under 77,000 cases in the first six months of 2023 a 43 per cent increase compared to the same period in 2022. Losses increased by 31 per cent to £40.9 million during the same period. Purchase scams are where people make a payment for goods that they believe to be genuine, but which never materialise. Purchase scams account for 66 per cent of all APP cases reported but only 17 per cent of total losses in the first half of 2023, evidencing the fact that typically purchase scams result in lower values losses than the other scam types.

In addition, investment scams also remain an area of concern. Despite the slight reduction in the first half of 2023 (down two per cent to £57.2 million) investment scams still account for nearly a quarter of all APP losses reported; the largest proportion of all APP scam types. This is where people are persuaded to transfer or 'invest' often substantial sums of money with tales of fictitious dividend payments or high returns, only to lose their investments.

A common factor behind all these scams is the criminals' use of online platforms, mobile phone networks and social media to target their victims and trick them into making payments. This includes fraudulent advertising on search engines, fake websites, and posts on social media. UK Finance has begun collecting and collating data on the origination of APP fraud which shows that 77 per cent of all APP scams during 2023 originated on an online platform of some description. This demonstrates the scale of fraud initiated outside of banks controls.

As we have warned previously, the level of fraud in the UK has reached a point where it must be considered a national security threat. Criminal gangs with technological know-how have long since realised that they can bypass the advanced security measures banks have in place and instead attempt to directly target the customer, usually outside the confines of the banking system. It is crucial that different sectors work together to fight fraud, which remains an ever growing and persistent threat to businesses, consumers, and the economy as a whole.

THE INDUSTRY RESPONSE:

The financial services sector is working hard to protect customers from fraud, including partnering with other sectors, government, and law enforcement to prevent and disrupt this criminal activity and bring its perpetrators to justice. The industry is responding to this threat by:

1. Working with the government and regulators to ensure the legislative framework supports a robust response to fraud. We have been engaging with government and parliamentarians on the progression of legislation, most recently in relation to the Online Safety Bill, Financial Services and Markets Act and Economic Crime and Corporate Transparency Bill.
2. Working with government on the recently published second Economic Crime Plan ('the Plan'). The Plan is outcomes-focused and reflects the shared aim of directing public-private resource towards agreed priorities to maximise collective action against the threat of economic crime. For the first time, fraud was included within the scope of the Plan with one of the outcomes being to cut fraud against individuals and businesses.
3. Supporting the government on its new Fraud Strategy with responses to several consultations on areas such as the ban on cold calling, sim farms and the computer Misuse Act, to help identify the impact of fraud and understand how consumers are manipulated in other environments. The industry has also been involved in the delivery of commitments in the Retail Banking Fraud Charter.
4. Co-chairing the Online Fraud Group, a joint public-private initiative that brings together senior representatives from the tech sector, financial services and law enforcement to take collective action to disrupt criminals.
5. Sharing intelligence on emerging threats with law enforcement, government departments and regulators through the National Economic Crime Centre. This drives down serious organised economic crime, protecting the public and safeguarding the prosperity and reputation of the UK as a financial centre.
6. The creation of the Dedicated Card and Payment Crime Unit (DCPCU), which was established in 2002, as a unique, proactive and fully operational police unit with a national remit, formed as a collaboration between UK Finance, the City of London Police and the Metropolitan Police Service.
    - In 2022 a three-year funding stream was secured to enable the Dedicated Card and Payment Crime Unit DCPCU to build a team to tackle emerging cryptocurrency cyber enabled threats. This new team helped the unit achieve industry savings of over £22 million from January to June alone.
7. Sharing intelligence across the banking and finance industry on emerging threats, data breaches and compromised card details via UK Finance's Intelligence and Information Unit ('I&I Unit'). In H1 1,064,503 compromised card numbers were received through law enforcement and disseminated by the I&I Unit to enable card issuers to take the necessary precautions to protect customers.
    - It is hoped that the new information sharing provisions within the Economic Crime and Corporate Transparency Bill will better enable the regulated sector to share information across a wide spectrum of economic crime, further strengthening the industry's ability to identify and mitigate threats
8. The continuation of initiatives across industries to share specific data and intelligence that mitigates live scam attacks including impersonation calls and SMS, as well as blocking high risk advertisements.

9. Continuing to work with the regulator Ofcom to crack down on number spoofing through the 'do not originate' list and inputting into their consultation on a potential solution to spoofing. This work has already resulted in ongoing protection for financial institutions, preventing criminals from spoofing the phone numbers of trusted organisations including those on the back of bank cards.

10. Working with text message providers and law enforcement to block scam text messages. Over 3,000 unauthorised sender IDs are currently being blocked to prevent them being used to send scam text messages mimicking trusted organisations.

11. Training employees to spot and stop suspicious transactions. The Banking Protocol rapid response scheme allows staff at banks, building societies and Post Offices to alert the police when they think a customer is being scammed, whether in branch, on the telephone, or through online banking. The Banking Protocol has prevented over £282.3 million in fraud and led to 1,298 arrests since it launched in 2016. In 2023 from January to June £24.1 million worth of fraud losses were stopped through the scheme.

12. Delivering customer education campaigns to help people stay safe from fraud, spot the signs of a scam, and prevent consumers being duped by criminals. These include the Take Five to Stop Fraud and Don't Be Fooled campaigns. 38 major banks and building societies have signed up to the Take Five Charter, bringing the industry together to give people simple and consistent fraud awareness advice.

13. Specific education and awareness in schools through the Don't be Fooled campaign, which worked with education specialists iChild to create a free education resource pack for primary and secondary school pupils to educate and deter them from becoming a money mule.

14. Undertaking continual analysis and consumer research to understand what constitutes effective warnings against fraud for customers, looking for impactful ways to highlight the risks, increase protections and encourage preventative actions through the payment journey.

15. Continually working with independent vendors and payment schemes to develop innovative tools to enable firms to identify fraud risk and track funds where fraudulent payments are made.

16. Working with industry to develop secure data sharing solutions to enable real time sharing of information when a fraud has occurred. This enables firms to freeze funds and repatriate to the rightful owner and in doing so limiting the financial gain of criminal entities. For example, UK Finance's Best Practice Standards System record real time information when an APP fraud occurs, including the 'enablers' of the fraud outside of the payment system.

17. The creation of a voluntary industry code for the reimbursement of victims of authorised push payment scams. The Contingent Reimbursement Model ('CRM') Code set out new consumer protection standards to reduce APP scams and give victims more consistent treatment and reimbursement. We are now working with the Payment Systems Regulator (PSR) on delivering proposals for a new reimbursement regime to include the entire financial industry and ensure consistent consumer outcomes.

18. The creation of a National Fraud Database, funded by the industry, which provides a comprehensive database of fraud risk data and intelligence. Hundreds of thousands of records are added every year by the UK's fraud prevention community. The data and intelligence is shared in real time and online: 24 hours a day, seven days a week.

TOTAL UNAUTHORISED FRAUD (CARDS, CHEQUES AND REMOTE BANKING)

	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Prevented	£821.7m	£1005.6m	£852.5m	£763.2m	£733.0m	£632.1m	£590.6m	£577.5m	£650.7m	**10%**
Cases	1,385,486	1,406,825	1,383,352	1,527,157	1,496,840	1,415,627	1,397,765	1,383,546	1,260,194	**-10%**
Gross Loss	£408.4m	£416.4m	£374.0m	£409.8m	£397.3m	£333.0m	£352.4m	£374.5m	£340.7m	**-3%**

Losses due to unauthorised transactions on cards, cheques and remote banking decreased to £340.7 million in the first half of this year, down three per cent on the same period in the previous year.

The number of recorded cases of unauthorised fraud fell by ten per cent to 1.26 million.

There was a rise of ten per cent in the value of prevented fraud in H1 2023, with banks stopping £650.7 million of unauthorised fraudulent transactions. This equates to the industry preventing £6.56 in every £10 of attempted fraud.

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

TOTAL AUTHORISED PUSH PAYMENT FRAUD

NOTE: APP DATA PRIOR TO 2020 IS NOT DIRECTLY COMPARABLE AND IT IS THEREFORE EXCLUDED FROM THIS PUBLICATION

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Cases	69,093	85,521	101,540	94,456	95,167	112,205	116,324	**22%**
Payments	105,069	139,502	172,622	172,515	166,327	205,939	211,558	**27%**
Gross Loss	£188.1m	£232.6m	£301.5m	£281.8m	£241.9m	£243.3m	£239.3m	**-1%**
Returned to Victim	£75.0m	£99.7m	£125.8m	£131.9m	£135.6m	£150.0m	£152.8m	**13%**

Losses due to authorised push payment scams were £239.3 million in the first six months of 2023.

This was split between personal (£196.7 million) and non-personal or business (£42.6 million). In total there were 116,324 cases. Of this total, 112,459 cases were on personal accounts and 3,865 cases were on non-personal accounts.

In total £152.8 million was returned to victims in H1 2023 or 64 per cent of the total loss. This has increased by 13 per cent (from £135.6 million) in H1 2022, which amounted to 54 per cent of all losses being returned to the victim.

UNAUTHORISED PAYMENT CARD FRAUD

	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Prevented	£489.5m	£518.0m	£486.8m	£496.5m	£481.7m	£484.9m	£492.0m	£482.2m	£546.2m	**11%**
Cases	1,365,112	1,380,427	1,352,646	1,482,976	1,444,996	1,378,206	1,371,469	1,361,403	1,241,326	**-9%**
Gross Loss	£313.3m	£307.3m	£287.9m	£286.4m	£261.3m	£263.2m	£270.2m	£286.0m	£258.9m	**-4%**

This covers fraud on debit, credit, charge, and ATM-only cards issued in the UK.

Payment card fraud losses are organised into five categories:

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

Fraud losses on cards totalled £258.9 million in the first half of 2023, a decrease of four per cent on the same period in 2022.

Over this period, the overall value of card spending grew by 8.7 per cent. Card fraud as a proportion of card purchases has decreased from 7.1p per £100 in the first half of 2022 to 6.5p per £100 in the first half of 2023. A total of £546 million of card fraud was stopped by banks and card companies in the first six months of 2023. This is equivalent to £6.78 in every £10 of attempted card fraud prevented without a loss occurring.

REMOTE PURCHASE (CARD NOT PRESENT)

	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Cases	1,071,493	1,085,925	1,134,399	1,283,467	1,264,562	1,159,264	1,136,886	1,084,140	980,289	**-14%**
Gross Loss	£237.4m	£232.8m	£222.8m	£229.8m	£210.1m	£202.4m	£198.1m	£197.6m	£173.8m	**-12%**

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 12 per cent to £173.8 million in the first six months of 2023; the lowest total reported for eight years (since 2015). The number of cases fell by 14 per cent to just over 980,000; the first time case volumes have dropped below 1 million since 2018. The reductions in remote purchase can be attributed to the implementation of PSD2 (Strong Customer Authentication) and the adoption of One-Time Passcodes (OTPs)

Intelligence suggests remote purchase fraud continues to result mainly from criminals using card details obtained through data theft, such as third-party data breaches and via phishing emails and scam text messages. Criminals are also taking advantage of the increasing tendency for online shoppers to search for discounted items on social media platforms. When a customer goes to buy the product advertised from 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.

"Digital skimming" is another method criminals use to steal card data from customers when they shop online. In a typical digital skimming attack, criminals will add malicious code to the online retailer's website which steals sensitive information including card details at the check-out stage. This information is then sent to a domain controlled by criminals, who use it to commit remote purchase fraud.

These attacks highlight the importance of online retailers maintaining robust security measures, including by ensuring payment platforms are regularly updated with the latest software. Strong Customer Authentication (SCA) in the context of e-commerce has now taken effect as demonstrated by the reductions in this type of fraud. SCA rules are aimed at reducing fraud by verifying a customer's identity when they make certain online purchases.

However, to circumvent these additional protections, criminals are increasingly using social engineering techniques to trick customers into divulging their OTPs so they can authenticate fraudulent online card transactions. Customers are also being tricked by criminals into making online card transactions themselves, mimicking authorised push payments.

OTPs should be treated with caution, in the same way as your PIN, and consumers should only contact businesses and retailers on a number they know to be genuine. Before entering your OTP for any transaction you must make sure you check that it accurately describes the transaction or purchase you're about to make. If you receive a code you weren't expecting, contact your bank immediately on a number you know to be genuine, such as the one listed on the back of your debit or credit card.

Contained within these figures, e-commerce card fraud totalled an estimated £151 million in the first half of 2023, a reduction of 15 per cent when compared with the same period in 2022.

How to stay safe from remote purchase fraud:

- If you're using an online retailer for the first time, always take time to research them before you give them any of your details. Be prepared to ask questions before making a payment.
- If an offer looks too good to be true then it probably is. Be suspicious of prices that are unusually low.
- Only use retailers you know and trust, for example, ones you know or have been recommended to you. If you're buying an item made by a major brand, you can often find a list of authorised sellers on their official website.
- Take a moment to install any built-in security technology most browsers offer.
- If you have visited a website you think is suspicious you can report it to the **National Cyber Security Centre**.
- Where possible, use a credit card when making purchases over £100 and up to £30,000 as you receive protection under Section 75 of the Consumer Credit Act.
- Always ensure you click 'log out' or 'sign out' of websites.

If you think you have been scammed, contact your bank immediately and report it to Action Fraud.

LOST AND STOLEN CARD FRAUD

	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Cases	230,727	229,415	166,710	155,284	144,713	180,788	185,609	215,731	188,333	**1%**
Gross Loss	£48.3m	£46.4m	£41.1m	£37.8m	£35.1m	£42.1m	£46.9m	£53.2m	£48.3m	**3%**

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 three per cent in 2023 and totalled £48.3 million. There was also a slight rise in the number of incidents reported, increasing one per cent to just over 188,000 cases.

After the rise in 2022 following the increase to contactless limits during the pandemic, fraud activity levelled out in the first six months of 2023 with losses and case volumes consistent with those seen in H1 2022. During the same period contactless spending has grown by 15 per cent totalling £135 billion, equating to around only 1.4 pence in every £100 spent using contactless technology being fraudulent. The industry continues to deploy a range of fraud prevention and detection tools to protect consumers from contactless card fraud and these tools remain highly effective in the fight against this type of fraud. Each card has an inbuilt security feature which means that from time to time, cardholders making a contactless transaction will be asked to enter their PIN to prove they are in possession of their card. The frequency of this varies between card issuers.

How to stay safe from lost and stolen fraud:

- Always report any lost or stolen cards to your bank or card company straight away.
- Check your statements regularly and if you spot any payments you don't recognise, contact your bank or card company immediately.
- Make sure you fully cover your PIN whenever you enter it.

If you think you have been scammed, contact your bank immediately and report it to Action Fraud.

CARD NOT RECEIVED

	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Cases	3,949	3,958	4,193	4,242	4,126	4,815	5,093	3,755	2,876	**-44%**
Gross Loss	£2.5m	£2.7m	£2.1m	£2.3m	£2.0m	£2.0m	£1.9m	£2.0m	£1.4m	**-29%**

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 29 per cent to £1.4 million during January to June 2023; the lowest total ever recorded for this loss type, case volumes fell by 44 per cent in the same period; also the lowest ever reported total.

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.

How to stay safe from card not received fraud:

- If you are expecting a new card and it hasn't arrived, call your bank or card company for an update.
- Tell your bank or card company immediately if you move home. Use the Royal Mail redirection service to redirect your post to your new address for at least a year.
- Be extra vigilant if you live in a property where other people may have access to your mail, such as a block of flats. In some cases, your bank or card company can arrange for you to collect your cards from a local branch or building society.

If you think you have been scammed, contact your bank immediately and report it to Action Fraud.

COUNTERFEIT CARD FRAUD

	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Cases	30,980	34,927	28,389	24,393	14,640	10,268	9,664	9,930	8,624	**-11%**
Gross Loss	£6.6m	£6.2m	£5.4m	£3.3m	£2.6m	£2.1m	£2.2m	£2.5m	£2.3m	**7%**

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 2023, a rise of less than seven per cent compared with H1 2022. Case volumes fell by 11 per cent to 8,624, the lowest total since data collection began.

To obtain the data required to create a counterfeit card, criminals attach concealed or disguised devices to the card-reader slots of ATMs and unattended payment terminals, 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 criminals' use of the counterfeit cards.

How to stay safe from counterfeit card fraud:

- Make sure you fully cover your PIN whenever you enter it.
- If you spot anything suspicious at an ATM or an unattended payment terminal, or someone is watching you, then do not use the machine and report it to your bank.
- Check your statements regularly and if you spot any payments you don't recognise, contact your bank or card company immediately.

If you think you have been scammed, contact your bank immediately and report it to Action Fraud.

CARD ID THEFT

	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Cases	27,963	26,202	18,955	15,590	16,955	23,071	34,217	47,847	61,204	**79%**
Gross Loss	£18.5m	£19.2m	£16.5m	£13.2m	£11.5m	£14.7m	£21.1m	£30.6m	£33.1m	**57%**

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 57 per cent in the first six months of 2023 compared with the same period in 2022, from £21.1 million to £33.1 million. The number of individual cases also increased significantly over the same period, rising by 79 per cent to 61,204 cases; both totals are the highest ever recorded for this category.

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 that the increase behind this type of fraud is a result of criminals' 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.

How to stay safe from card ID fraud:

- Use a redirection service when moving to a new home such as the one provided by the Royal Mail as well as informing your bank, card company and other organisations of your new address.
- Destroy unwanted documents including bills, bank statements or post that is received in your name, preferably by using a shredder.
- Request copies of your personal credit report from a credit reference agency on a regular basis to check for any entries you don't recognise.
- Provide as little personal information about yourself on social media as possible and only accept requests to connect from people you know.
- You can apply to be on the Cifas Protective Registration Service for a fee which places a flag next to your name and personal details in their secure National Fraud Database. Companies and organisations who have signed up as members of the database can see you're at risk and take extra steps to protect you, preventing criminals from using your details to apply for products or services.

- Be careful if other people have access to your post. Contact Royal Mail if you think your post is being stolen. Cancel any lost or stolen credit or debit cards immediately.
- Keep your personal information secure when using your card over the phone, on the internet, or in shops by ensuring that others can't overhear you or see your information.
- If your passport, driving licence, cards or other personal information has been lost or stolen, immediately contact the organisation that issued it.

Criminals may use the identity of a deceased person to commit identity theft. If someone close to you passes you can protect their identity using the **Deceased Preference Service**.

If you think you have been scammed, contact your bank immediately and report it to Action Fraud.

FURTHER CARD FRAUD ANALYSIS

PLEASE NOTE: Figures in the following sections relate to the places where the card was used fraudulently, rather than how the card or the card details were compromised. This is simply another way of breaking down 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. For example, 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 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Gross Loss	£32.4m	£31.9m	£25.5m	£23.3m	£19.6m	£27.3m	£33.3m	£38.8m	£38.2m	**14%**

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

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

UK CASH MACHINE FRAUD

	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Gross Loss	£15.5m	£14.5m	£15.0m	£13.1m	£12.0m	£12.4m	£12.9m	£13.2m	£12.6m	**-2%**

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 PIN and card.

Losses at UK cash machines decreased by two per cent in the first half of 2023, compared with the same period in 2022.

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

UK / INTERNATIONAL CARD FRAUD

	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
UK Gross Loss	£229.3m	£220.6m	£208.5m	£206.0m	£187.6m	£196.4m	£202.4m	£213.8m	£196.5m	**-3%**
Int Gross Loss	£84.0m	£86.7m	£79.4m	£80.4m	£73.7m	£66.8m	£67.9m	£72.2m	£62.5m	**-8%**

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

Both categories decreased in the first half of 2023, UK card fraud losses by three per cent to £196.5 million and international fraud losses by eight per cent, to £62.5 million.

CHEQUE FRAUD

	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Prevented	£202.3m	£348.5m	£184.2m	£54.3m	£21.0m	£12.0m	£10.5m	£9.3m	£5.5m	**-47%**
Cases	1,515	1,337	709	538	382	433	415	551	560	**35%**
Gross Loss	£29.4m	£24.2m	£6.4m	£5.8m	£3.5m	£2.9m	£3.2m	£4.3m	£2.9m	**-10%**

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 a 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 ten per cent in the first half of 2023, while the number of cases rose 35 per cent to 560 cases.

It should be noted that the volume and value of cheque fraud remains very low, and while increases have been reported in 2023, they are not considered to be significant.

How to stay safe from cheque fraud:

- Always complete cheques using a ballpoint pen, or pen with indelible ink.
- Draw a line through all unused spaces, including after the payee's name.
- Keep your chequebook in a safe place and report any missing cheques to your bank immediately.
- Check your statements regularly and if you spot any payments you don't recognise, contact your bank or building society immediately.
- Wait for cheques to clear before despatching goods or providing services.

If you think you have been scammed, contact your bank immediately and report it to Action Fraud.

REMOTE BANKING FRAUD

	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Prevented	£129.8m	£139.1m	£181.5m	£212.3m	£230.3m	£135.3m	£88.1m	£86.0m	£99.0m	**12%**
Cases	18,859	25,061	29,997	43,643	51,462	36,988	25,881	21,592	18,308	**-29%**
Gross Loss	£65.7m	£84.9m	£79.7m	£117.6m	£132.5m	£67.0m	£78.9m	£84.2m	£78.9m	**0%**

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 was £78.9 million in the first half of 2023, the same amount as that lost in the first six months of 2022. The number of cases of remote banking fraud decreased, falling by 29 per cent to 18,308.

It is worth noting that this type of fraud peaked during the Covid-19 pandemic in 2021 (£132.5 million) and the reduction seen in 2022 and 2023 was expected as lockdown restrictions eased.

UK Finance research shows that last year, 86 per cent of the adult population used at least one form of remote banking.

A total of £99 million of attempted remote banking fraud was stopped by bank security systems in the first six months of 2023. This is equivalent to 55p in every £1 of fraud attempted being prevented.

In addition, 12 per cent (£19.9 million) of the losses across all remote banking channels were recovered after the incident.

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

INTERNET BANKING

	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Cases	10,409	15,440	21,312	34,683	42,628	29,929	18,001	14,035	8,826	**-51%**
Gross Loss	£48.8m	£63.1m	£64.3m	£95.4m	£108.0m	£50.3m	£55.5m	£58.6m	£53.4m	**-4%**

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 login details. This includes using impersonation scam calls, emails or text messages typically exploiting current affairs (energy bill discounts, cost-of-living support, etc) 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 2023, falling four per cent to £53.4 million when compared with the same period in 2022. Case volumes also reduced, falling by 51 per cent to 8,826.

£9.8 million (18 per cent) of these losses across internet banking fraud were recovered after the incident.

How to stay safe from internet banking fraud:

- A genuine bank or organisation will never contact you to ask for your full PIN or passwords. Only give out your personal or financial details to use a service to which you have given your consent, that you trust and which you are expecting to be contacted by.
- Always question uninvited approaches in case it's a scam. Instead, contact the company directly using a known email or phone number.
- Don't be tricked into giving a criminal access to your personal or financial details. Never automatically click on links in emails or texts.
- Ensure you have the most up-to-date security software installed on your computer, including anti-virus. Some banks offer free security software, so check your bank's website for details.

If you think you have been scammed, contact your bank immediately and report it to Action Fraud.

TELEPHONE BANKING FRAUD

	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Cases	5,504	5,695	4,681	2,809	2,545	2,078	1,776	1,300	1,404	**-21%**
Gross Loss	£11.6m	£12.0m	£7.9m	£8.1m	£7.5m	£8.0m	£7.4m	£7.3m	£6.8m	**-8%**

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 eight per cent to £6.8 million in the first six months of 2023, the lowest recorded total since we began collecting data for this fraud type in 2012. The number of cases decreased by 21 per cent to 1,404.

In addition, 11 per cent (£0.8 million) of the losses across the telephone banking channel were recovered after the incident.

How to stay safe from telephone banking fraud:

- Never disclose security details, such as your full banking password. A genuine financial provider or organisation will never ask you for these in an email, on the phone, by message or in writing.
- Never give remote access to any of your devices while on a phone call as criminals may then be able to log in to your online banking.
- Always question uninvited approaches for your personal or financial information in case it's a scam. Instead, contact the company directly using a known email or phone number.
- Don't assume the person on the phone or emailing you is who they say they are. Just because someone knows your basic details (such as your name and address, your mother's maiden name, or even your direct debits), it doesn't mean they are genuine.
- Your bank or the police will never ask you to transfer money to a safe account.
- You can forward suspicious emails to **report@phishing.gov.uk** and suspected scam texts to your mobile network provider by forwarding them to 7726. An easy way to remember 7726 is that they are the numbers on your telephone keypad that spell out the word 'SPAM'. Phone numbers operating scam calls can be reported by texting 'CALL' to 7726 and following the prompts.
- If you have visited a website you think is suspicious you can report it to the **National Cyber Security Centre**.

If you think you have been scammed, contact your bank immediately and report it to Action Fraud.

MOBILE BANKING FRAUD

	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Cases	2,946	3,926	4,004	6,151	6,289	4,981	6,104	6,257	8,078	**32%**
Gross Loss	£5.3m	£9.9m	£7.5m	£14.0m	£17.1m	£8.7m	£16.0m	£18.2m	£18.7m	**17%**

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.

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 53 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, and this is likely to continue rising as people become more familiar and comfortable with mobile banking, and the functionality offered through mobile banking improves and payment limits increase.

Losses from mobile banking fraud increased by 17 per cent to £18.7 million in the first six months of 2023, the highest recorded total since we began collecting data for this fraud type in 2015. The number of cases increased by 32 per cent to 8,078 also the highest total recorded.

In addition, five per cent (£1 million) of the losses across telephone banking were recovered after the incident.

How to stay safe from mobile banking fraud:

- Don't be tricked into giving a criminal access to your personal or financial information. Never automatically click on links in unexpected emails or messages and always question uninvited approaches.
- Be wary of messages that encourage you urgently to visit a website or call a number to verify or update your details.
- If you have visited a website you think is suspicious you can report it to the **National Cyber Security Centre**.
- Always question uninvited approaches in case it is a scam. Instead, contact the company directly using a known email or phone number.

If you think you have been scammed, contact your bank immediately and report it to Action Fraud.

AUTHORISED PUSH PAYMENT FRAUD

In an Authorised Push Payment (APP) scam, a criminal will trick their victim into sending money directly from their account to an account which the criminal controls.

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

APP fraud losses continue to be driven by criminals' abuse of online platforms to scam their victims. This includes investment scams advertised on search engines and social media, romance scams committed via online dating platforms and purchase scams promoted through auction websites. Once the victim has authorised the payment and the money has reached the criminal's account, the criminal will quickly transfer the money out to numerous other accounts, often abroad, where it is then cashed out.

This can make it difficult for banks to trace the stolen money. However, the industry has worked with Pay.UK to implement new technology that helps track suspicious payments and identify money mule accounts. If a customer authorises the payment themselves, current legislation means that they have no legal protection to cover them for losses – which is different to unauthorised transactions. Nevertheless 64 per cent of losses (£152.8 million) were returned/refunded to customers in H1 2023. The Payment Systems Regulator (PSR) is currently consulting on proposals that would require payment service providers to reimburse losses in all but exceptional cases.

		H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
PERSONAL	**Cases**	66,291	78,916	98,102	90,862	92,186	108,457	112,459	**22%**
	Payments	100,977	127,969	167,003	166,748	161,680	200,081	205,470	**27%**
	Loss	£151.9m	£195.5m	£261.8m	£244.1m	£203.0m	£205.2m	£196.7m	**-3%**
	Return to customer	£63.5m	£85.4m	£112.6m	£120.8m	£120.2m	£133.9m	£136.4m	**13%**
NON-PERSONAL	**Cases**	2,802	6,605	3,438	3,594	2,981	3,748	3,865	**30%**
	Payments	4,092	11,533	5,619	5,767	4,647	5,858	6,088	**31%**
	Loss	£36.2m	£37.1m	£39.6m	£37.7m	£38.9m	£38.1m	£42.6m	**10%**
	Return to customer	£11.5m	£14.3m	£13.2m	£11.1m	£15.4m	£16.1m	£16.5m	**7%**
OVERALL	**Cases**	69,093	85,521	101,540	94,456	95,167	112,205	116,324	**22%**
	Payments	105,069	139,502	172,622	172,515	166,327	205,939	211,558	**27%**
	Loss	£188.1m	£232.6m	£301.4m	£281.8m	£241.9m	£243.3m	£239.3m	**-1%**
	Return to customer	£75.0m	£99.7m	£125.8m	£131.9m	£135.6m	£150.0m	£152.8m	**13%**

Losses due to APP scams were £239.3 million in the first six months of 2023, a decrease of one per cent when compared with the same period in 2022. This was split between personal (£196.7 million) and non-personal (£42.6 million). In total there were 116,324 cases of APP fraud reported in January to June 2023 (112,459 personal and 3,865 non-personal), an increase of 22 per cent on the same period in 2022. The fact that case volumes have increased whilst losses have reduced shows that criminals prefer lower value purchase scams to reach an increased audience on online platforms rather than specifically targeting victims for higher value frauds.

FRAUD ORIGINATION

Our annual reporting of fraud statistics draws information from banks and payment service providers on identified and reported fraudulent activity. It concentrates on the prevalence and nature of different fraud and scam types, as well as the losses incurred. This enables the industry and stakeholders to monitor change over time, informing ongoing detection and prevention strategies.

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

UK Finance is publishing data which sheds new light on the source of Authorised Push Payment (APP) fraud. We can do this through analysis of a subset of APP data which uses anonymised case data that includes insight on the reported origination of fraud events.

This shows that:

- 77 per cent of fraud cases originate from online sources. These cases tend to include lower-value scams such as purchase fraud and therefore account for 32 per cent of total losses.
- 17 per cent of fraud cases originate from telecommunications, these are usually higher value cases such as impersonation scams and so account for 45 per cent of losses.

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

	H1 2023	
	VOLUME	VALUE
Online	77%	32%
Telecommunications	17%	45%
Email	1%	11%
Other	5%	12%

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 'authorised 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 chance of being able to freeze it and stop it ending up in a criminal's hands.

- UK Finance has access to aggregate reporting from the BPS system, allowing it to assess the volume and value of fraud and scams and the origination of the fraudulent activity, as reported by the victim. Aggregate information is compiled only once members have investigated the fraudulent activity and cases are closed. UK Finance does not have access to individual case information and is therefore unable to make an assessment as to the accuracy of the data included, and no quality assurance checks are undertaken on the data inputs. However, extensive testing, engagement with members during the development of the system, and validation with other sources of fraud data allows the conclusion that the extracted data are consistent with industry trends.
- The data presented provide a statement of the origination of fraud and scams during the stated periods, noting that the victim will not, in every case, be aware of where the initial compromise happened, and as such these figures cannot be considered definitive. Only information relating to cases that have been closed are loaded to the BPS platform, so not all incidents of scams will be included here. For more detail on these please refer to the UK Finance Annual Fraud Report.
- Data may be subject to future restatement if further information becomes available.

APP VOLUNTARY CODE

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

UK Finance collates and publishes statistics relating to the cases assessed using the voluntary code. Data show that 107,413 cases have been assessed and closed during H1 2023, with a total value of £187.4 million. Of this, £128.7 million was reimbursed to victims (69 per cent of the total). Of the 86,937 cases reported, 81 per cent involved values of less than £1,000, whilst only three per cent of cases involved the more life-changing sums of £10,000 plus.

		H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Less than £1k	**Cases**	49,992	54,347	66,820	60,591	64,086	77,860	86,937	**36%**
	Payments	62,220	68,438	84,320	81,205	87,357	108,826	123,466	**41%**
	Loss	£13.1m	£16.5m	£20.3m	£17.6m	£16.3m	£19.6m	£20.0m	**23%**
	Returned to Victim	£4.4m	£5.5m	£7.4m	£7.8m	£10.1m	£13.6m	£15.2m	**50%**
£1k-£10k	**Cases**	12,583	18,326	24,793	22,343	20,661	21,775	17,314	**-16%**
	Payments	25,970	39,428	57,457	50,966	46,844	54,359	48,126	**3%**
	Loss	£41.2m	£60.6m	£80.3m	£68.7m	£62.9m	£63.9m	£52.8m	**-16%**
	Returned to Victim	£17.8m	£27.6m	£36.6m	£33.6m	£37.9m	£39.8m	£33.6m	**-11%**
Over 10k	**Cases**	2,657	3,355	4,497	4,001	3,149	3,322	3,162	**0%**
	Payments	8,760	13,181	18,693	21,966	19,562	24,590	23,597	**21%**
	Loss	£84.8m	£99.8m	£142.1m	£140.4m	£117.3m	£108.0m	£114.6m	**-2%**
	Returned to Victim	£40.0m	£49.1m	£70.9m	£70.3m	£69.2m	£68.5m	£79.9m	**15%**
OVERALL	**Cases**	65,232	76,028	96,110	86,935	87,896	102,957	107,413	**22%**
	Payments	96,950	121,047	160,470	154,137	153,763	187,775	195,189	**27%**
	Loss	£139.1m	£176.9m	£242.7m	£226.7m	£196.6m	£191.6m	£187.4m	**-5%**
	Returned to Victim	£62.2m	£82.3m	£114.9m	£111.7m	£117.2m	£121.9m	£128.7m	**10%**

FURTHER ANALYSIS OF THE APP SCAM DATA

UK Finance collates enhanced data which provide further insight into APP scams.

This data covers:

- Eight scam types: malicious payee (purchase scam, investment scam, romance scam and advance fee scam) and malicious redirection (invoice and mandate scam, CEO fraud, impersonation: police/bank staff, and impersonation: other).
- Six payment types: faster payment, CHAPS, BACS (payment), BACS (standing order), intrabank ("on-us") and international.
- Four payment channels: branch, internet banking, telephone banking and mobile banking. The data in the following sections provide a breakdown of the overall APP scam data detailed in the previous section and are not in addition to the total figures. Included within each scam type is the data relating to the cases which have been assessed using the APP voluntary code.

APP SCAM TYPES

PURCHASE SCAM

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Cases	40,486	43,806	50,327	49,406	53,907	63,263	76,946	**43%**
Payments	50,933	56,560	64,948	67,463	72,282	86,836	107,660	**49%**
Loss	£23.9m	£27.2m	£32.3m	£31.8m	£31.1m	£35.9m	£40.9m	**31%**
Returned to Victim	£6.5m	£8.1m	£9.3m	£11.7m	£16.5m	£21.6m	£25.7m	**56%**

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 Authorised Push Payment (APP) scam with 76,946 confirmed cases accounting for two thirds of the total number of all APP scam cases reported in the first half of 2023. A total of £40.9 million was lost to purchase scams during the same period; both totals (volume and value) are now at their highest point since we began collecting data in 2020.

Payment Service Providers (PSP) returned £25.7 million (63 per cent) of the losses to the victims.

VOLUNTARY CODE: PURCHASE SCAM ONLY

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

	Less than £1k	£1k-£10k	More than £10k	Total
Cases	65,717	5,937	334	71,988
Payments	86,736	12,820	1,307	100,863
Loss	£12.4m	£16.8m	£7.5m	£36.7m
Returned to Victim	£9.5m	£9.1m	£4.5m	£23.0m

For those cases which were applicable for assessment using the voluntary code during the first half of 2023, 63 per cent of all losses were returned to the victim compared with 51 per cent in the same period for 2022. 91 per cent of all cases assessed involved case values of less than £1,000.

How to stay safe from purchase scams:

- Be suspicious of any offers or prices that look too good to be true.
- Always use the secure payment method recommended by reputable online retailers and auction websites. Be very wary of requests to pay by bank transfer.
- Always do your research and ask questions before you buy. Ask to see any vehicle in person first and request the relevant documentation to ensure the seller owns it.
- If you're buying an item made by a major brand, you can often find a list of authorised sellers on their official website.
- Contact your bank immediately if you think you may have fallen for a purchase scam.
- Where possible, use a credit card when making purchases over £100 and up to £30,000 as you receive protection under Section 75 of the Consumer Credit Act.

If you think you have been scammed, contact your bank immediately and report it to Action Fraud.

INVESTMENT SCAM

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Cases	3,655	4,526	6,224	5,850	5,161	4,924	5,112	**-1%**
Payments	8,720	11,203	17,567	18,098	14,928	15,583	16,936	**13%**
Loss	£47.6m	£61.8m	£90.6m	£81.1m	£58.4m	£55.7m	£57.2m	**-2%**
Returned to Victim	£14.2m	£22.6m	£34.8m	£37.0m	£29.4m	£29.2m	£33.5m	**14%**

In an investment scam, a criminal convinces their victim to move their money to a fictitious fund or to pay for a fake investment. The criminal will usually promise a high return to entice their victim into making the transfer. These scams include investment in items such as gold, property, carbon credits, cryptocurrencies, land banks and wine.

The criminals behind investment scams often use cold-calling to target their victim and pressurise them to act quickly by claiming the opportunity is time limited. Adverts on social media usually offering unrealistic returns, and letters are also used heavily in investment scams.

Investment scam losses decreased by two per cent in January to June 2023 to £57.2 million. After the peak seen in 2021 during the pandemic losses and case volumes have levelled out, this is likely a combination of factors including fewer opportunities for criminal(s) to contact victims now that lockdown restrictions have eased, and also the emergence of cost-of-living pressures meaning individuals are more cautious with money and less likely to be looking for investment opportunities.

Investment scams continued to account for the largest value of all eight Authorised Push Payment (APP) scam types with losses of £57.2 million or 24 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 five per cent of the total number of APP scam cases.

Payment Service Providers (PSP) returned £33.5 million (59 per cent) of the losses to the victims up from 50 per cent in the first half of 2022.

VOLUNTARY CODE: INVESTMENT SCAM ONLY

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

	Less than £1k	£1k-£10k	More than £10k	Total
Cases	2,406	1,252	775	4,433
Payments	4,419	4,447	5,741	14,607
Loss	£0.8m	£4.6m	£38.1m	£43.4m
Returned to Victim	£0.5m	£2.6m	£23.3m	£26.4m

For those cases which were applicable for assessment using the voluntary code during the first half of 2023, 61 per cent of all losses were returned to the victim compared with 56 per cent in the same period for 2022.

How to stay safe from investment scams:

- Be cautious of approaches presenting you with exclusive investment opportunities. It could be a scam if you're being pressurised to act quickly.
- Most cryptocurrencies aren't regulated by the Financial Conduct Authority (FCA), which means they're not protected by the UK's Financial Services Compensation Scheme. It's important that you do your research and proceed with extreme caution before making any investments.
- Check the FCA's register for regulated firms, individuals, and bodies. You can check their website is genuine by checking their web address. It should always begin with fca.org.uk or register.fca.org.uk. Ensure you only use the contact details listed on the Register to confirm you're dealing with the genuine firm before parting with your money and information.
- You can check if an investment or pension opportunity you've been offered could potentially be a scam by taking the FCA's ScamSmart test.
- Report scam ads appearing in paid-for space online by visiting the Advertising Standard Authority's website where you can complete their quick reporting form.

If you think you have been scammed, contact your bank immediately and report it to Action Fraud.

ROMANCE SCAM

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Cases	1,107	1,218	1,479	1,791	1,644	2,005	2,120	**29%**
Payments	6,051	7,134	11,489	14,325	13,199	17,021	18,889	**43%**
Loss	£8.5m	£9.3m	£12.7m	£18.2m	£14.6m	£16.7m	£18.5m	**26%**
Returned to Victim	£2.9m	£3.1m	£4.3m	£7.8m	£7.2m	£9.3m	£11.6m	**62%**

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.

Criminals 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 £18.5 million was lost to romance scams during January to June 2023, an increase of 26 per cent when compared with the same period in 2022. In this scam type, victims are often convinced to make multiple, generally smaller, payments to the criminal over a longer period of time compared to other fraud types. As a result, romance scams have an average of nearly nine scam payments per case; the highest of the eight scam types. Victims of cases committed during lockdown (when APP fraud was at its highest) may only now be realising that they have been duped and therefore reporting it to their bank.

Payment Services Providers (PSP) were subsequently able to return £11.6 million to victims or 63 per cent of the total, an increase from the 49 per cent being reimbursed during the same period in 2022.

VOLUNTARY CODE: ROMANCE SCAM ONLY

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

	Less than £1k	£1k-£10k	More than £10k	Total
Cases	912	654	310	1,876
Payments	3,161	6,595	7,299	17,055
Loss	£0.3m	£2.3m	£12.0m	£14.6m
Returned to Victim	£0.2m	£1.6m	£8.0m	£9.8m

For those cases which were applicable for assessment using the voluntary code during the first half of 2023, 67 per cent of all losses were returned to the victim compared with 50 per cent in the same period for 2022.

How to stay safe from romance scams:

- Avoid sending money to someone you've never met in person, particularly if you have only recently met online.
- Research the person you're talking to as profile photos may not be genuine. You can do this by uploading a picture of the person you're talking to into search engines to check that profile photos are not associated with another name.
- Be alert to spelling and grammar mistakes and inconsistencies in stories.
- Stay on the dating site or on the messaging service until you're confident the person is who they say they are and ensure meetings in person take place in public.
- Always consider the possibility of a scam.
- Only accept friend requests from people you know and trust.
- Speak to your family or friends to get advice.

If you think you have been scammed, contact your bank immediately and report it to Action Fraud.

ADVANCE FEE SCAM

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Cases	5,697	8,136	9,064	11,431	11,472	15,857	12,239	**7%**
Payments	9,245	13,987	16,233	20,737	20,609	30,622	27,049	**31%**
Loss	£8.3m	£13.9m	£14.1m	£18.1m	£14.2m	£18.0m	£15.1m	**6%**
Returned to Victim	£3.0m	£4.5m	£5.3m	£6.1m	£6.3m	£11.5m	£9.6m	**52%**

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 second most common form of Authorised Push Payment (APP) scam in the first half of 2023, accounting for 11 per cent of the total number of cases. A total of £15.1million was lost to advance fee scams, an increase of six percent compared with the first six months of 2022.

Payment Service Providers (PSP) returned £9.6 million (64 per cent) of the losses to the victims up from 44 per cent in the first half of 2022.

VOLUNTARY CODE: ADVANCE FEE SCAM ONLY

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

	Less than £1k	£1k-£10k	More than £10k	Total
Cases	9,621	1,574	218	11,413
Payments	17,334	5,836	2,229	25,399
Loss	£2.4m	£4.1m	£6.6m	£13.1m
Returned to Victim	£1.9m	£2.4m	£4.1m	£8.4m

For those cases which were applicable for assessment using the voluntary code during the first half of 2023, 64 per cent of all losses were returned to the victim compared with 41 per cent in the same period for 2022.

How to stay safe from advance fee scams:

- Question claims that you are due money for goods or services that you haven't ordered or are unaware of, especially if you have to pay any fees upfront.
- It's extremely unlikely that you've won a lottery or competition that you haven't entered, and which requires an upfront fee.

- Check the email address of recruiters or employers to ensure they're genuine and be vigilant of those platforms that businesses would be unlikely to use i.e. Yahoo, Hotmail or Gmail.
- Confirm organisations you're being contacted by are registered on Companies House and use the details provided to contact recruitment companies and other organisations directly. You can check their website is genuine by checking their web address.
- Be suspicious of fake profiles on social media platforms, for example LinkedIn offering jobs that don't exist.
- Make sure you use a reputable recruitment company who are a member of a trade association such as the REC, APSCo and TEAM. You can check this by looking for the association's logos on the company's website or by visiting the trade association's website directly and searching by member.
- If you're concerned about a job scam you can report it to a trade association and to SAFERjobs using their online reporting tool.

If you think you have been scammed, contact your bank immediately and report it to Action Fraud.

INVOICE AND MANDATE SCAM

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Cases	2,778	1,943	2,053	2,277	1,591	1,749	1,665	**5%**
Payments	3,613	2,707	2,813	3,354	2,340	2,625	2,352	**1%**
Loss	£40.1m	£28.6m	£27.1m	£29.6m	£25.5m	£24.0m	£24.8m	**-2%**
Returned to Victim	£16.5m	£13.3m	£10.8m	£11.7m	£13.6m	£12.8m	£12.2m	**-11%**

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 £24.8 million in the first half of 2023, a decrease of two per cent when compared with the same period in 2022.

71 per cent (£17.4 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 (PSP) returned £12.2 million (49 per cent) of the losses to the victims down from 53 per cent in the first half of 2022. Invoice and mandate scam is one of only two scam types to show a decrease in reimbursement rate in H1 2023.

VOLUNTARY CODE: INVOICE AND MANDATE SCAM ONLY

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

	Less than £1k	£1k-£10k	More than £10k	Total
Cases	351	561	211	1,123
Payments	441	762	409	1,612
Loss	£0.2m	£2.1m	£7.9m	£10.2m
Returned to Victim	£0.1m	£1.4m	£5.9m	£7.5m

For those cases which were applicable for assessment using the voluntary code during the first half of 2023, 74 per cent of all losses were returned to the victim compared with 56 per cent in the same period for 2022.

How to stay safe from invoice and mandate scams:

- Always confirm any bank account details directly with a company either on the telephone or in person before you make any changes, a payment or transfer/pay any money.
- Criminals can access or alter emails to make them look genuine. Do not use the contact details in an email, instead check the company's official website or documentation.
- If you are making a payment to an account for the first time, transfer a small sum first and then check with the company using known contact details that the payment has been received to check the account details are correct.

If you think you have been scammed, contact your bank immediately and report it to Action Fraud.

- Where possible, send confirmation of payment to service providers once their invoice has been paid
- Always question changes in payment information. Companies rarely change their bank details
- Be careful what you share on social media as criminals may target you if they know the next step is a large financial transaction

CEO SCAM

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Cases	187	170	230	231	200	232	196	**-2%**
Payments	235	252	331	347	297	318	302	**2%**
Loss	£2.4m	£2.4m	£6.1m	£6.6m	£7.9m	£5.6m	£6.9m	**-13%**
Returned to Victim	£1.1m	£0.7m	£1.6m	£1.2m	£2.2m	£1.4m	£1.3m	**-38%**

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 Authorised Push Payment (APP) scam in H1 2023, accounting for less than one per cent of total cases. A total of £6.9 million was lost, equivalent to only three per cent of total APP losses. CEO has the highest average case value of all eight scam types with an average of just under £35,000 being lost per confirmed case.

Payment Service Providers (PSP) returned £1.3 million (20 per cent) of the losses to the victims down from 28 per cent in the first half of 2022. The CEO scam is one of only two scam types to show a decrease in reimbursement rate in H1 2023. However given the low values associated with this category, it should be noted that one large case can significantly impact percentage changes.

VOLUNTARY CODE: CEO SCAM ONLY

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

	Less than £1k	£1k-£10k	More than £10k	Total
Cases	8	51	19	78
Payments	11	63	46	120
Loss	£3,336	£0.3m	£0.5m	£0.8m
Returned to Victim	£2150	£0.2m	£0.3m	£0.4m

For those cases which were applicable for assessment using the voluntary code during the first half of 2023, 55 per cent of all losses were returned to the victim compared with 38 per cent in the same period for 2022.

How to stay safe from CEO scams:

- Always check unusual payment requests directly, ideally in person or by telephone, to confirm the instruction is genuine. Do not use contact details from an email, message or letter.

- Establish documented internal processes for requesting and authorising all payments and be suspicious of any request to make a payment outside of the company's standard process.
- Be cautious of unexpected emails, messages or letters which request urgent bank transfers, even if the message appears to have originated from someone from your own organisation.
- If you receive a message asking you to purchase vouchers or goods always check in person or by telephone that the instruction you have received is genuine.

If you think you have been scammed, contact your bank immediately and report it to Action Fraud.

IMPERSONATION: POLICE OR BANK STAFF

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Cases	7,983	13,194	17,521	11,885	9,138	7,810	5,979	-35%
Payments	14,049	26,548	34,774	28,032	22,533	25,997	17,911	-21%
Loss	£34.7m	£56.1m	£75.6m	£61.8m	£59.4m	£50.4m	£43.5m	-27%
Returned to Victim	£20.0m	£32.1m	£40.6m	£38.6m	£42.0m	£40.4m	£35.0m	-17%

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 18 per cent of all Authorised Push Payment (APP) scam losses in H1 2023 totalling £43.5 million. However, losses have decreased by 27 per cent when compared with the same period in 2022 and case volumes have fallen by 35 per cent in the same period. This is likely to be a result of the decreased opportunities for criminals to contact victims since lockdown restrictions were lifted and 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 seen in the past 18-24 months.

Payment Service Providers (PSP) were able to return £35 million of the losses to customers or 80 per cent of the total; the highest reimbursement rate of all eight scam types and an increase from the 71 per cent reimbursed in H1 2022.

VOLUNTARY CODE: IMPERSONATION: POLICE OR BANK STAFF ONLY

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

	Less than £1k	£1k-£10k	More than £10k	Total
Cases	1,849	2,623	996	5,468
Payments	3,508	8,689	4,822	17,019
Loss	£0.7m	£10.4m	£28.4m	£39.5m
Returned to Victim	£0.6m	£8.2m	£22.2m	£31.1m

For those cases which were applicable for assessment using the voluntary code during the first half of 2023, 79 per cent of all losses were returned to the victim compared with 71 per cent in the same period for 2022.

How to stay safe from impersonation scams:

- Your bank or the police will never ask you to transfer money to a safe account.
- Only give out your personal or financial information to services you have consented to and are expecting to be contacted by.
- Always contact your bank, card company or an organisation directly using a known email or phone number.
- Never give anyone remote access to your computer following a cold call, email or unsolicited message.
- You can forward suspicious emails to report@phishing.gov.uk and suspected scam texts to your mobile network provider by forwarding them to 7726. If a scam text claims to be from your bank, then you should also report it to them.
- HMRC will never notify you about tax refunds, penalties or ask for your personal or financial information through emails, texts or phone calls. You can forward suspicious emails claiming to be from HMRC to phishing@hmrc.gov.uk and texts to 60599.
- HMRC will never call threatening arrest. Any offers of tax refunds or requests for financial information should also be treated with caution. You can forward suspicious emails claiming to be from HMRC to **phishing@hmrc.gov.uk** and texts to 60599. If you're unsure whether it's a scam, check their guidance on recognising scams, and for more detail on reporting methods visit gov.uk.

If you have visited a website you think is suspicious you can report it to the National Cyber Security Centre.

Only criminals will ask you to lie to your bank.

IMPERSONATION: OTHER

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Cases	7,200	12,528	14,642	11,585	12,054	16,365	12,067	**0%**
Payments	12,223	21,111	24,467	20,159	20,139	26,937	20,459	**2%**
Loss	£22.5m	£33.3m	£43.0m	£34.6m	£30.8m	£37.0m	£32.6m	**6%**
Returned to Victim	£10.8m	£15.3m	£19.2m	£17.7m	£18.5m	£23.8m	£23.9m	**29%**

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 £32.6 million was lost to this type of scam during the first six months of 2023, an increase of six per cent when compared with 2022.

Payment Service Providers (PSP) were able to return £23.9 million of the losses to customers or 71 per cent of the total.

VOLUNTARY CODE: IMPERSONATION: OTHER ONLY

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

	Less than £1k	£1k-£10k	More than £10k	Total
Cases	6,073	4,662	299	11,034
Payments	7,856	8,914	1,744	18,514
Loss	£3.2m	£12.2m	£13.5m	£28.9m
Returned to Victim	£2.3m	£8.1m	£11.5m	£22.0m

For those cases which were applicable for assessment using the voluntary code during the first half of 2023, 76 per cent of all losses were returned to the victim compared with 61 per cent in the same period for 2022.

How to stay safe from other impersonation scams:

- Always question uninvited approaches in case it's a scam. Instead, contact the company directly using a known email or phone number.
- Criminals may have some details about you, however just because someone knows your basic details it does not mean they are genuine.
- Never give anyone remote access to your computer as the result of a cold call, email or unsolicited message.

If you think you have been scammed, contact your bank immediately and report it to Action Fraud.

PAYMENT TYPE

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

Values	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Faster Payment	£149.3m	£200.1m	£263.7m	£240.8m	£208.3m	£212.8m	£199.1m	**-4%**
CHAPS	£8.2m	£6.3m	£9.3m	£13.2m	£8.8m	£5.1m	£13.1m	**49%**
BACS	£15.1m	£8.4m	£11.1m	£9.3m	£12.5m	£11.4m	£13.2m	**6%**
Intra Bank Transfer	£2.7m	£7.9m	£5.3m	£2.3m	£0.5m	£1.1m	£1.6m	**244%**
International	£12.9m	£9.9m	£12.2m	£16.2m	£11.8m	£12.9m	£12.3m	**4%**
Total	£188.1m	£232.6m	£301.5m	£281.8m	£241.9m	£243.3m	£239.3m	**-1%**

Volumes	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Faster Payment	101,297	135,344	167,720	167,731	163,142	201,822	207,957	**27%**
CHAPS	244	257	435	329	398	152	196	**-51%**
BACS	667	526	729	966	911	1,316	1,284	**41%**
Intra Bank Transfer	1,402	1,711	2,100	1,258	532	710	812	**53%**
International	1,459	1,664	1,638	2,231	1,344	1,939	1,309	**-3%**
Total	105,069	139,502	172,622	172,515	166,327	205,939	211,558	**27%**

PAYMENT CHANNEL

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

Values	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Branch	£19.7m	£23.9m	£27.2m	£29.3m	£25.0m	£20.7m	£27.5m	**10%**
Internet Banking	£126.8m	£135.7m	£171.4m	£157.7m	£135.6m	£139.0m	£129.5m	**-4%**
Telephone Banking	£9.7m	£8.1m	£11.3m	£13.1m	£8.7m	£6.9m	£7.7m	**-12%**
Mobile Banking	£32.0m	£64.8m	£91.5m	£81.7m	£72.5m	£76.8m	£74.7m	**3%**
Total	£188.1m	£232.6m	£301.5m	£281.8m	£241.9m	£243.3m	£239.3m	**-1%**

Volume	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
Branch	3,445	5,523	4,070	4,181	3,754	4,811	4,482	**19%**
Internet Banking	55,608	58,245	62,789	67,227	63,229	75,471	72,368	**14%**
Telephone Banking	2,687	2,906	2,725	3,524	3,203	2,973	3,710	**16%**
Mobile Banking	43,329	72,828	103,038	97,583	96,141	122,668	130,998	**36%**
Total	105,069	139,502	172,622	172,515	166,327	205,923	211,558	**27%**

LIST OF MEMBERS WHO HAVE CONTRIBUTED DATA TO THIS PUBLICATION

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

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.

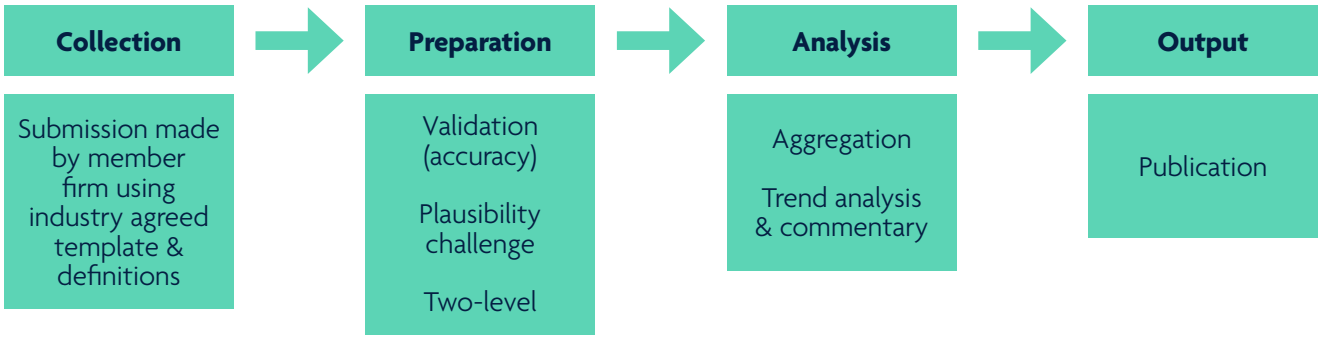
Data plausibility – inputs

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.

APPENDIX

CASES

TYPE	CATEGORY	SUB CATEGORY	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
UNAUTHORISED	CARD	Lost & stolen	166,710	155,284	144,713	180,788	185,609	215,731	188,333	**1%**
UNAUTHORISED	CARD	CNR	4,193	4,242	4,126	4,815	5,093	3,755	2,876	**-44%**
UNAUTHORISED	CARD	Counterfeit	28,389	24,393	14,640	10,268	9,664	9,930	8,624	**-11%**
UNAUTHORISED	CARD	Remote purchase	1,134,399	1,283,467	1,264,562	1,159,264	1,136,886	1,084,140	980,289	**-14%**
UNAUTHORISED	CARD	Card ID Theft	18,955	15,590	16,955	23,071	34,217	47,847	61,204	**79%**
UNAUTHORISED	CHEQUE	Cheque	709	538	382	433	415	551	560	**35%**
UNAUTHORISED	REMOTE BANKING	Internet Banking	21,312	34,683	42,628	29,929	18,001	14,035	8,826	**-51%**
UNAUTHORISED	REMOTE BANKING	Tel Banking	4,681	2,809	2,545	2,078	1,776	1,300	1,404	**-21%**
UNAUTHORISED	REMOTE BANKING	Mobile Banking	4,004	6,151	6,289	4,981	6,104	6,257	8,078	**32%**
AUTHORISED	PAYMENT	Invoice & Mandate	2,778	1,943	2,053	2,277	1,591	1,749	1,665	**5%**
AUTHORISED	PAYMENT	CEO	187	170	230	231	200	232	196	**-2%**
AUTHORISED	PAYMENT	IMP: Police/Bank	7,983	13,194	17,521	11,885	9,138	7,810	5,979	**-35%**
AUTHORISED	PAYMENT	IMP: Other	7,200	12,528	14,642	11,585	12,054	16,365	12,067	**0%**
AUTHORISED	PAYMENT	Purchase	40,486	43,806	50,327	49,406	53,907	63,263	76,946	**43%**
AUTHORISED	PAYMENT	Investment	3,655	4,526	6,224	5,850	5,161	4,924	5,112	**-1%**
AUTHORISED	PAYMENT	Romance	1,107	1,218	1,479	1,791	1,644	2,005	2,120	**29%**
AUTHORISED	PAYMENT	Advance Fee	5,697	8,136	9,064	11,431	11,472	15,857	12,239	**7%**

LOSSES

TYPE	CATEGORY	SUB CATEGORY	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H2 2022	H1 2023	CHANGE 22-23
UNAUTHORISED	CARD	Lost & stolen	£41.1m	£37.8m	£35.1m	£42.1m	£46.9m	£53.2m	£48.3m	**3%**
UNAUTHORISED	CARD	CNR	£2.1m	£2.3m	£2.0m	£2.0m	£1.9m	£2.0m	£1.4m	**-29%**
UNAUTHORISED	CARD	Counterfeit	£5.4m	£3.3m	£2.6m	£2.1m	£2.2m	£2.5m	£2.3m	**7%**
UNAUTHORISED	CARD	Remote purchase	£222.8m	£229.8m	£210.1m	£202.4m	£198.1m	£197.6m	£173.8m	**-12%**
UNAUTHORISED	CARD	Card ID Theft	£16.5m	£13.2m	£11.5m	£14.7m	£21.1m	£30.6m	£33.1m	**57%**
UNAUTHORISED	CHEQUE	Cheque	£6.4m	£5.8m	£3.5m	£2.9m	£3.2m	£4.3m	£2.9m	**-10%**
UNAUTHORISED	REMOTE BANKING	Internet Banking	£64.3m	£95.4m	£108.0m	£50.3m	£55.5m	£58.6m	£53.4m	**-4%**
UNAUTHORISED	REMOTE BANKING	Tel Banking	£7.9m	£8.1m	£7.5m	£8.0m	£7.4m	£7.3m	£6.8m	**-8%**
UNAUTHORISED	REMOTE BANKING	Mobile Banking	£7.5m	£14.0m	£17.1m	£8.7m	£16.0m	£18.2m	£18.7m	**17%**
AUTHORISED	PAYMENT	Invoice & Mandate	£40.1m	£28.6m	£27.1m	£29.6m	£25.5m	£24.0m	£24.8m	**-2%**
AUTHORISED	PAYMENT	CEO	£2.4m	£2.4m	£6.1m	£6.6m	£7.9m	£5.6m	£6.9m	**-13%**
AUTHORISED	PAYMENT	IMP: Police/ Bank	£34.7m	£56.1m	£75.6m	£61.8m	£59.4m	£50.4m	£43.5m	**-27%**
AUTHORISED	PAYMENT	IMP: Other	£22.5m	£33.3m	£43.0m	£34.6m	£30.8m	£37.0m	£32.6m	**6%**
AUTHORISED	PAYMENT	Purchase	£23.9m	£27.2m	£32.3m	£31.8m	£31.1m	£35.9m	£40.9m	**31%**
AUTHORISED	PAYMENT	Investment	£47.6m	£61.8m	£90.6m	£81.1m	£58.4m	£55.7m	£57.2m	**-2%**
AUTHORISED	PAYMENT	Romance	£8.5m	£9.3m	£12.7m	£18.2m	£14.6m	£16.7m	£18.5m	**26%**
AUTHORISED	PAYMENT	Advance Fee	£8.3m	£13.9m	£14.1m	£18.1m	£14.2m	£18.0m	£15.1m	**6%**