UK FINANCE

2022 HALF YEAR FRAUD UPDATE

In association with:

LexisNexis® RISK SOLUTIONS

ukfinance.org.uk

INTRODUCTION

The figures released by UK Finance show that after the rises in fraud to record highs during the pandemic, fraud levels fell in the first half of this year (2022) as consumers return to normal routines. Nonetheless, criminals continue to look for new ways to exploit potential victims as fraud continues to evolve.

In the first half of this year, criminals stole a total of £609.8 million through authorised and unauthorised fraud and scams, a decrease of just under 13 per cent compared to H1 2021. The advanced security systems used by banks also prevented just under £584 million from being stolen.

During the first half of 2022 criminals have continued to focus activity mainly on socially engineering their victims, usually with the intention of tricking them into authorising a payment to an account within their control (known as Authorised Push Payment (APP) Fraud).

The tactics that criminals use 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 authorise payments.

While APP fraud has fallen in the first half of 2022 compared to the same period 2021 (down 17 per cent to £249 million) it is still more than 30 per cent higher than the same period in 2020 and remains a focus for the banking and finance industry.

Despite the overall decrease in fraud levels, romance scam losses increased by almost a third (31 per cent) in the first half of 2022. This is where the victim is persuaded to make a payment to a person they have met, often online through social media and with whom they believe they are in a relationship.

Meanwhile, there has also been an increase in the number of purchase scams, although the total value of losses due to these scams fell. This is where people make a payment for goods that they believe to be genuine, but which never materialise. Purchase scams account for 56 per cent of all APP scams reported in the first half of 2022.

In addition, investment scams also remain an area of considerable concern, still accounting for the largest proportion of losses of all eight APP scam types despite a 32 per cent fall in losses. 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 fraudsters' use of online platforms 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.

It is concerning that there has also been a significant increase in online user generated posts encouraging people to become money mules – where people allow their bank account to be used to 'cash out' fraudulent funds. These posts are typically aimed at younger people who may not realise the severity of what they are doing or even know that it is a crime. While it is difficult to determine how much of the fraud losses are passing through money mule networks, it is clear that these money mule accounts enable criminals to get away with fraud. It is far more difficult for banks to identify transactions such as these, because the money is being passed through existing and legitimate accounts.

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. The importance of different sectors working together to fight fraud remains a crucial part of our weaponry to tackle what is an ever growing and persistent threat to businesses, consumers and the economy as a whole.

The banking and finance industry continues to invest billions in tackling fraud. However, the banking sector cannot solve this on its own. There must be a coordinated approach adopted across every sector if this is to be tackled effectively.

THE INDUSTRY RESPONSE

The banking and finance industry is working hard to protect customers from fraud and scams, while partnering with government, law enforcement and the private sector to catch and prosecute the criminal gangs responsible.

It is responding to this threat by:

- Investing in advanced security systems to protect customers from fraud, including realtime transaction analysis. The industry prevented £583.9 million of unauthorised fraud in the first half of 2022, equivalent to 61.8p in every £1 of attempted unauthorised fraud being stopped without a loss occurring.

- Working with the government and law enforcement to establish clear strategic priorities, improve accountability and coordination through the Economic Crime Strategic Board (ECSB), jointly chaired by the home secretary and the chancellor. The ECSB has agreed a number of public private priorities, with a focus on Suspicious Activity Reports (SARs) Reform, work on legislative proposals and effectiveness and efficiency.

- The jointly published Home Office and UK Finance Economic Crime Plan sets out how to better harness the combined capabilities of the public and private sectors to make the UK a leader in the global fight against economic crime. The industry is working with the government on a new Economic Crime Plan and Ten-Year Fraud Strategy. The Economic Crime and Corporate Transparency Bill currently before Parliament will support this by providing a framework for all sectors working together.

- 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.

- 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 the first half of 2022, 1.04 million compromised card numbers were received through law enforcement and disseminated via the I&I unit to enable card issuers to take the necessary precautions to protect customers. The industry has proposed new powers on information and intelligence sharing to make it easier for regulated sector firms to share information with each other.

- Delivering customer education campaigns to help them stay safe from fraud, spot the signs of a scam, and to prevent consumers being duped by criminals. These include our Take Five to Stop Fraud and Don't Be Fooled campaigns. 36 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.

- Training staff 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 online banking. The Banking Protocol has prevented £230.1 million in fraud and led to 1,079 arrests since it launched in 2016. In the first half of 2022 alone, £27.4 million was stopped through the scheme.

- Sponsoring a specialist police unit, the Dedicated Card and Payment Crime Unit, which tackles the organised criminal groups responsible for financial fraud and scams. In 2021 the DCPCU prevented a record £101 million from being stolen, the highest amount in the unit's 20-year history.

- Working with the regulator Ofcom to crack down on number spoofing, including the development and enhancements of the 'do not originate' list. This work has led to significant successes in preventing criminals from spoofing the phone numbers of trusted organisations such as the numbers on the back of bank cards.
- Working with text message providers and law enforcement to block scam text messages. 2456 unauthorised sender IDs are currently being blocked to prevent them being used to send scam text messages mimicking trusted organisations.

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.

DRIVERS BEHIND THE FIGURES

While the end of the pandemic has seen falls in some types of fraud, others have increased as criminals continue to adapt their methods. While it is not possible to be specific about the values that can be attributed to individual methods of attack, intelligence reported by our members highlights the main drivers.

Social engineering, in which criminals groom and manipulate people into divulging personal or financial details or transferring money, continued to be the key driver of both unauthorised and authorised fraud losses in the first half of 2022. Criminals used scam phone calls, text messages and emails, as well as fake websites and social media posts, to trick people into handing over personal details and passwords. This information is then used to target victims and convince them to make payments to the criminal.

Investment scams remain high with significant associated losses. The scams are heavily enabled by fraudulent advertising on search engines and social media. There have been many reported cases of criminals impersonating private banks and investment firms. Victims may be cold called by fraudsters, while others have left their details on clone sites during online searches for investment opportunities. Scammers are also increasingly using social media sites to entice victims by advertising fake investments, such as crypto currency schemes or gold or property. In some cases, social media 'influencers' may be used to promote such schemes and create an air of legitimacy.

Fraud losses are also being driven by the theft of customers' personal and financial data, which often occurs because of data breaches in third parties and industries outside the financial sector.

Criminals also steal data by intercepting mail or inserting malware on customers' devices. This data is then used by criminals to carry out direct fraud, for example, by applying for a credit card in the victim's name or buying goods or services online using the stolen data.

Criminals are also deploying 'digital skimmers' 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 the criminals and often resold to fraudsters, who use it to commit remote purchase fraud. These attacks continue to highlight the importance of implementing and maintaining robust security measures within the online retail eco-system.

TOTAL UNAUTHORISED FRAUD

(Cards, Cheques and Remote Banking)

UNAUTHORISED	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 / H1 21 CHANGE
Prevented	£717.6m	£944.7m	£821.7m	£1005.6m	£852.5m	£763.2m	£733.0m	£632.1m	£583.9m	-20%
Cases	1,198,130	1,453,426	1,385,486	1,406,825	1,383,352	1,527,157	1,491,840	1,415,627	1,395,157	-7%
Gross Loss	£400.0m	£444.8m	£408.4m	£416.4m	£374.0m	£409.8m	£397.3m	£333.0m	£360.8m	-9%

Losses due to unauthorised transactions on cards, cheques and remote banking decreased to £360.8 million in the first half of this year, down nine per cent on the previous year.

The number of recorded cases of unauthorised fraud fell by seven per cent to just under 1.4 million. There was a fall of 20 per cent in the value of prevented fraud in H1 2022, with banks stopping £583.9 million of unauthorised fraudulent transactions. This equates to the industry preventing £6.18 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 is therefore excluded from this publication

APP	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 /H1 21 CHANGE
Cases	69,093	85,521	101,540	94,456	95,219	-6%
Gross Loss	£188.1m	£232.6m	£301.5m	£281.8m	£249.1m	-17%
Returned to victim	£75.0m	£99.7m	£125.8m	£131.9m	£140.1m	11%

Total losses due to authorised push payment scams decreased to £249.1 million in the first half of 2022, a fall of 17 per cent compared to the same period in 2021. The number of cases decreased by six per cent to 95,219.

There has been an increase in the amount returned to victims, from 42 per cent in the first half of 2021, to 56 per cent in the first six months of 2022. 30 per cent of cases were decided in under a week.

UNAUTHORISED PAYMENT CARD FRAUD

CARDS	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 /H1 21 CHANGE
Prevented	£501.4m	£625.0m	£489.5m	£518.0m	£486.8m	£496.5m	£481.7m	£484.9m	£480.0m	0%
Cases	1,181,533	1,436,206	1,365,112	1,380,427	1,352,646	1,482,976	1,444,996	1,378,206	1,365,618	-5%
Gross Loss	£305.7m	£365.7m	£313.3m	£307.3m	£287.9m	£286.4m	£261.3m	£263.2m	£272.3m	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 and card ID theft.

Fraud losses on cards totalled £272.3 million in the first half of 2022, an increase of four per cent on the same period in 2021.

Over this period, overall value of card spending grew by 14 per cent. Card fraud as a proportion of card purchases has decreased from 7.6p in the first half of 2021 to 7.1p in the first half of 2022.

A total of £480 million of card fraud was stopped by banks and card companies in the first six months of 2022. This is equivalent to £6.39 in every £10 of attempted card fraud prevented without a loss occurring.

REMOTE PURCHASE FRAUD

(Card not present)

CNP	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 /H1 21 CHANGE
Cases	922,515	1,127,760	1,071,493	1,085,925	1,134,399	1,283,467	1,264,562	1,159,264	1,131,704	-11%
Gross Loss	£231.8m	£274.6m	£237.4m	£232.8m	£222.8m	£229.8m	£210.1m	£202.4m	£199.4m	-5%

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 six per cent to £199.4 million in the first six months of 2022. The number of cases fell by 11 per cent, evidencing that card issuers are identifying and stopping individual incidents more swiftly.

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. 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.

"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 continue to highlight the importance of online retailers maintaining robust security measures, including by ensuring payment platforms are regularly updated with the latest software.

In March 2022, requirements for Strong Customer Authentication (SCA) in the context of e-commerce took effect. This follows the managed programme which UK Finance led on behalf of members in order to ensure an orderly migration to SCA. SCA rules are aimed at reducing fraud by verifying a customer's identity when they make certain higher-value online purchases. To circumvent these additional protections, criminals are increasingly using social engineering techniques to trick customers into divulging their One Time Passcodes (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.

One Time Passcodes (OTPs) should be treated in the same way as your PIN in that they should never be shared with anyone, including your bank. Before entering your OTP make sure you check 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 correct, 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 2022, a reduction of 15 per cent when compared to the same period in 2021.

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.
- Use the secure payment method recommended by reputable online retailers and auction sites.
- 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 Credit Consumer Act.
- If an offer looks too good to true then it probably is. Be suspicious of prices that are unusually low.
- Only use retailers you 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 the time to install the built-in security measures most browsers offer.

LOST AND STOLEN CARD FRAUD

LOST and STOLEN	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 /H1 21 CHANGE
Cases	204,862	230,129	230,727	229,415	166,710	155,284	144,713	180,788	185,039	28%
Gross Loss	£45.5m	£49.6m	£48.3m	£46.4m	£41.1m	£37.8m	£35.1m	£42.1m	£47.2m	35%

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.

Losses from this form of fraud increased by 35 per cent in H1 of this year. The number of incidents also increased by 28 per cent in the same period, compared to H1 2021.

As in previous updates, the intelligence reported to UK Finance suggests that as the industry introduces ever more sophisticated methods of fraud prevention, criminals are continuing to fall back on low-tech methods such as distraction thefts and card entrapment at ATMs, while distraction thefts are also now taking place at unattended payment terminals such as those in car parks.

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 then contact your bank or card company immediately.
- When making payments, make sure you fully cover your PIN with your free hand, purse or wallet whenever you enter it.

CARD NOT RECEIVED FRAUD

CNR	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 /H1 21 CHANGE
Cases	4,697	5,349	3,949	3,958	4,193	4,242	4,126	4,815	5,092	23%
Gross Loss	£3.0m	£3.3m	£2.5m	£2.7m	£2.1m	£2.3m	£2.0m	£2.0m	£2.0m	4%

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

Card not received fraud losses rose by four per cent the first six months of 2022 to £2 million, while the number of individual cases increased by 23 per cent.

Criminals typically target multi-occupancy buildings such as flats to carry out 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 issuer immediately if you move home. Ask Royal Mail to redirect your post to your new address for at least a year.
- Be extra careful if you live in a property where other people have access to your mail, such as a block of flats. In some cases, your card company may arrange for you to collect your cards from a local branch.

COUNTERFEIT CARD FRAUD

COUNTERFEIT	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 / H1 21 CHANGE
Cases	28,109	30,527	30,980	34,927	28,389	24,393	14,640	10,268	9,669	-34%
Gross Loss	£7.9m	£8.4m	£6.6m	£6.2m	£5.4m	£3.3m	£2.6m	£2.1m	£2.3m	-13%

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 the first six months of 2022, a fall of 13 per cent compared to 2021. Case volumes fell by a third, falling 34 per cent to just under 10,000. Both gross losses and case volumes have fallen to the lowest totals on record for this type of fraud.

To obtain the data required to create a counterfeit card, criminals attach concealed or disguised devices to the card-reader slots of ATMs and unattended payment terminals (UPTs), such as self-service ticket machines at railway stations, cinemas, and car parks.

The counterfeit cards are typically used overseas in countries yet to upgrade to Chip and PIN. The significant decrease in this type of fraud since 2008 is likely to be a result of the introduction of chip technology in the UK and its subsequent increased adoption around the world, most notably in the United States.

How to stay safe from counterfeit card fraud:

- Always protect your PIN by fully covering the keypad with your free hand, purse or wallet.
- If you spot anything suspicious at an ATM or 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 then contact your bank or card company immediately.

CARD ID THEFT

ID THEFT	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 /H1 21 CHANGE
Cases	21,350	42,441	27,963	26,202	18,955	15,590	16,955	23,071	34,114	101%
Gross Loss	£17.4m	£29.9m	£18.5m	£19.2m	£16.5m	£13.2m	£11.5m	£14.7m	£21.4m	86%

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 86 per cent in the first six months of 2022 compared to the same period in 2021, from £11.5 million to £21.4 million. The number of individual cases more than doubled over the same period.

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.

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 you have accounts with of your new address.
- Destroy unwanted documents including bills, bank statements or post that's 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 invitations 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 have 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.

FURTHER CARD FRAUD ANALYSIS

Figures in the following sections relate to the places where the card was fraudulently used, rather than how the card or card details were compromised. These figures provide a different breakdown of the overall payment card fraud totals and are not in addition to those in the previous sections.

Case volumes are not available for the place of misuse, to avoid double counting, as one case can cover multiple places of misuse. For example, a lost or stolen card could be used to make an ATM withdrawal and to purchase goods on the high street.

UK RETAIL FACE-TO-FACE FRAUD

UK FACE TO FACE	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 / H1 21 CHANGE
Gross Loss	£31.4m	£38.4m	£32.4m	£31.9m	£25.5m	£23.3m	£19.6m	£27.3m	£33.6m	72%

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.

Contactless fraud covers fraud on both contactless cards and mobile devices. Fraud on contactless cards and devices more than doubled in the first six months of 2022 totalling £15.4 million. However, spending via contactless cards also increased by 76 per cent to £117 billion during the same period, meaning that fraud as a proportion of overall spending contactless fraud remains low and equivalent to 1.5p in every £100 spent using contactless technology being fraudulent.

UK CASH MACHINE FRAUD

UK ATM	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 / H1 21 CHANGE
Gross Loss	£15.9m	£16.7m	£15.5m	£14.5m	£15.0m	£13.1m	£12.0m	£12.4m	£12.9m	8%

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

Losses at UK cash machines increased by eight per cent in the first half of 2022, compared to the same period in 2021. Most of this fraud is thought to be perpetuated through distraction thefts and card entrapment at ATMs, and the increase has been caused in the main by increased opportunities to commit these types of crimes now lockdown is over.

UK / INTERNATIONAL FRAUD

UK/INT	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 / H1 21 CHANGE
UK Gross Loss	£226.7m	£269.9m	£229.3m	£220.6m	£208.5m	£206.0m	£187.6m	£196.4	£203.9m	9%
INT Gross Loss	£79.0m	£95.8m	£84.0m	£86.7m	£79.4m	£80.4m	£73.7m	£66.8m	£68.5m	-7%

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

UK card fraud losses increased by nine per cent to £203.9 million in H1 of this year, compared to the same period in 2021. Meanwhile international fraud losses decreased by 7 per cent, to £68.5 million.

The roll out of Chip and PIN technology around the world has helped to keep levels relatively low, combined with widespread lockdowns because of the global pandemic.

CHEQUE FRAUD

CHEQUE	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 / H1 21 CHANGE
Prevented	£74.3m	£143.9m	£202.3m	£348.5m	£184.2m	£54.3m	£21.0m	£12.0m	£12.1m	-43%
Cases	682	1,338	1,515	1,337	709	538	382	433	437	14%
Gross Loss	£3.3m	£17.2m	£29.4m	£24.2m	£6.4m	£5.8m	£3.5m	£2.9m	£3.6m	3%

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

Counterfeit cheques are printed on non-bank paper to look exactly like genuine cheques and are drawn by a fraudster on genuine accounts.

Forged cheques are genuine cheques that have been stolen from an innocent customer and used by a fraudster with a forged signature.

Fraudulently altered cheques are genuine cheques that have been made out by the genuine customer but have been altered in some way by a criminal before being paid in, e.g. by changing the beneficiary's name or the amount of the cheque.

Losses from cheque fraud increased by three per cent in the first half of 2022, while the number of cases rose 14 per cent. It should be noted that volumes of cheque fraud remain very low.

The value of attempted cheque fraud prevented by the banks fell by 43 per cent to £12.1 million in the first half of 2022, equivalent to £7.70 in every £10 of attempted fraud prevented.

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.

REMOTE BANKING FRAUD

REMOTE BANKING	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 / H1 21 CHANGE
Prevented	£141.9m	£175.8m	£129.8m	£139.1m	£181.5m	£212.3m	£230.3m	£135.3m	£91.9m	-60%
Cases	15,915	15,882	18,859	25,061	29,997	43,643	51,462	36,988	29,102	-43%
Gross Loss	£91.0m	£61.8m	£65.7m	£84.9m	£79.7m	£117.6m	£132.5m	£67.0m	£84.8m	-36%

Remote banking fraud losses are organised into three categories: internet banking, telephone banking and mobile banking.

Fraud occurs when a criminal gains access to an individual's bank account through one of the three remote banking channels by using compromised personal details and passwords to make an unauthorised transfer of money from the victim's account.

Losses from remote banking fraud fell by 36 per cent in H1 2022, compared to the same period in 2021, to £84.8 million. Meanwhile the number of cases also fell, decreasing 43 per cent over the same period to 29,102.

A main driver behind the reduction is that this type of fraud would have been at its most prevalent during lockdown when many people would have been working from home, spending longer online, and doing more internet shopping, which provided criminals with greater opportunities to trick people into revealing their security information. These opportunities have therefore reduced as restrictions are eased and ways of living return to normal.

A total of £91.9 million of unauthorised remote banking fraud was prevented in the first six months of 2022, this is equivalent to £5.20 in every £10 of attempted fraud being prevented.

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

INTERNET BANKING	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 / H1 21 CHANGE
Cases	11,151	9,753	10,409	15,440	21,312	34,683	42,628	29,929	21,487	-50%
Gross Loss	£75.6m	£47.4m	£48.8m	£63.1m	£64.3m	£95.4m	£108.0m	£50.3m	£61.2m	-43%

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.

Fraudsters 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.

Losses from internet banking fell by 43 per cent to £61.2 million in the first six months of 2022, compared to the all-time high reported in H1 2021 of £108 million. The number of cases also decreased by 50 per cent, to 21,487. Again, these significant decreases reflect that this type of fraud would have been at its most prevalent during lockdown when many people would have been working from home, spending longer online, and doing more internet shopping which provided criminals with greater opportunities to trick people into revealing their security information. These opportunities have therefore reduced as restrictions are eased and ways of living return to normal.

£7.7 million (13 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 trusted organisation will never contact you out of the blue to ask for your full PIN, passwords or passcodes. Only give out your personal or financial details to use a service to which you have given your consent, that you trust and by which you are expecting to be contacted.
- 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 a link in an email or text.
- Ensure you have the most up-to-date security software installed on your computer, mobile or tablet, including anti-virus.

TELEPHONE BANKING FRAUD

TELEPHONE BANK	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 / H1 21 CHANGE
Cases	3,464	4,473	5,504	5,695	4,681	2,809	2,545	2,078	1,849	-27%
Gross Loss	£11.4m	£10.6m	£11.6m	£12.0m	£7.9m	£8.1m	£7.5m	£8.0m	£7.9m	6%

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

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

Losses from telephone banking fraud increased by six per cent to £7.9 million in the first six months of 2022, when compared to the same period in 2021. The number of cases decreased by 27 per cent, to 1,849.

In addition, eight per cent (£0.6 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 passwords or passcodes. A genuine financial provider or trusted organisation will never ask you for these in an email, on the phone 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 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.

MOBILE BANKING FRAUD

MOBILE BANK	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 /H1 21 CHANGE
Cases	1,300	1,656	2,946	3,926	4,004	6,151	6,289	4,981	5,766	-8%
Gross Loss	£4.0m	£3.8m	£5.3m	£9.9m	£7.5m	£14.0m	£17.1m	£8.7m	£15.7m	-8%

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

It excludes web browser banking on a mobile and browser-based banking apps (incidents on those platforms are included in the internet banking fraud figures).

Rises are to be expected in the mobile banking channel as the level of usage increases amongst customers and while losses have decreased slightly in comparison to H1 2021 they have increased in comparison to H2 2021. Around 60 per cent of adults living in the UK now use a mobile banking app either on their telephone or tablet, up from 33 per cent in 2015, and this is likely to continue rising as people become more familiar with and comfortable with mobile banking, and the functionality offered through mobile banking improves and payment limits increase.

Nine per cent (£1.4 million) of the losses across the mobile banking channel 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 emails or texts and always question uninvited approaches.
- Be wary of text messages that encourage you urgently to visit a website or call a number to verify or update your details.
- Always question uninvited approaches in case it's a scam. Instead, contact the company directly using a known email or phone number.

AUTHORISED PUSH PAYMENT FRAUD

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

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

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

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. 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	H1 22 / H1 21 CHANGE
PERSONAL	Cases	66,291	78,916	98,102	90,862	92,215	-6%
	Payments	100,977	127,969	167,003	166,748	162,906	-2%
	Loss	£151.9m	£195.5m	£261.8m	£244.1m	£208.6m	-20%
	Returned to Customer	£63.5m	£85.4m	£112.6m	£120.8m	£123.6m	10%
NON-PERSONAL	Cases	2,802	6,605	3,438	3,594	3,004	-13%
	Payments	4,092	11,533	5,619	5,767	4,669	-17%
	Loss	£36.2m	£37.1m	£39.6m	£37.7m	£40.5m	2%
	Returned to Customer	£11.5m	£14.3m	£13.2m	£11.1m	£16.5m	25%
OVERALL	Cases	69,093	85,521	101,540	94,456	95,219	-6%
	Payments	105,069	139,502	172,622	172,515	167,575	-3%
	Loss	£188.1m	£232.6m	£301.5m	£281.8m	£249.1m	-17%
	Returned to Customer	£75.0m	£99.7m	£125.8m	£131.9m	£140.1m	11%

Losses due to authorised push payment scams were £249.1 million in the first six months of 2022, a decrease of 17 per cent when compared to the same period in 2021. This was split between personal (£208.6 million) and non-personal or business (£40.5 million). In total there were 95,219 cases. Of this total, 92,215 cases were on personal accounts and 3,004 cases were on non-personal accounts.

Despite the overall decreases in APP fraud, the amount returned to customer has increased, rising by 11 per cent to £140.1million in the first half of 2022 or 56 per cent of the total loss.

APP VOLUNTARY CODE

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

UK Finance collates and publishes statistics relating to the cases assessed using the voluntary code. Data show that 87,896 cases have been assessed and closed during H1 2022, with a total value of £196.6 million. Of this, £117.2 million was reimbursed to victims (60 per cent of the total). Of the 87,896 cases reported, 73 per cent involved values of less than £1,000, while four per cent of cases involved the more life-changing sums of £10,000 plus.

APP CODE		H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 / H1 21 CHANGE
Less than £1k	Cases	49,992	54,347	66,820	60,591	64,086	-4%
	Payments	62,220	68,438	84,320	81,205	87,357	4%
	Loss	£13.1m	£16.5m	£20.3m	£17.6m	£16.3m	-20%
	Returned to Victim	£4.4m	£5.5m	£7.4m	£7.8m	£10.1m	37%
£1k-£10k	Cases	12,583	18,326	24,793	22,343	20,661	-17%
	Payments	25,970	39,428	57,457	50,966	46,844	-18%
	Loss	£41.2m	£60.6m	£80.3m	£68.7m	£62.9m	-22%
	Returned to Victim	£17.8m	£27.6m	£36.6m	£33.6m	£37.9m	3%
Over 10k	Cases	2,657	3,355	4,497	4,001	3,149	-30%
	Payments	8,760	13,181	18,693	21,966	19,562	5%
	Loss	£84.8m	£99.8m	£142.1m	£140.4m	£117.3m	-17%
	Returned to Victim	£40.0m	£49.1m	£70.9m	£70.3m	£69.2m	-2%
OVERALL	Cases	65,232	76,028	96,110	86,935	87,896	-9%
	Payments	96,950	121,047	160,470	154,137	153,763	-4%
	Loss	£139.1m	£176.9m	£242.7m	£226.7m	£196.6m	-19%
	Returned to Victim	£62.2m	£82.3m	£114.9m	£111.7m	£117.2m	2%

The finance industry is tackling authorised push payment scams by:

- Collaborating with telecommunications and technology companies to stop fraud at source before victims lose money.
- Working with domain registries to prevent fraudulent and cloned websites.
- Sharing data with other sectors to stop fraud before it reaches the financial sector.
- Sponsoring a specialist police unit, the Dedicated Card and Payment Crime Unit, which tackles the organised criminal groups responsible for financial fraud and scams. In 2021 the Unit prevented a record £101 million of fraud, the highest amount in its history.
- Collaborating with Pay.UK to improve data sharing within the payment journey to increase identification of fraudulent payments.
- Working with Pay.UK to implement the Mules Insights Tactical Solution (MITS), a new technology that helps to track suspicious payments and identify money mule accounts.
- Working with Pay.UK on the ongoing implementation of Confirmation of Payee, an account name checking service that helps to prevent authorised push payment scams, used when a payment is being made. This took effect in March 2022.
- Helping to prevent customers being duped by criminals by raising awareness of scams and how to stay safe through the Take Five to Stop Fraud and Don't Be Fooled campaigns.
- Delivering the Banking Protocol – a ground-breaking rapid response scheme through which staff in branches and call centres can alert police to suspected frauds taking place. The Protocol has prevented £230.1 million in fraud and led to 1,079 arrests since it launched in 2016. In the first half of 2022 alone, £27.4 million was stopped through the scheme.

FURTHER ANALYSIS OF THE APP SCAM DATA

UK Finance also collates enhanced data which provides 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, Internal transfer ("on-us") and International.
- Four payment channels: Branch, Internet Banking, Telephone Banking and Mobile Banking.

The data in the following sections provides a breakdown of the overall APP scam data detailed above and is not in addition to those figures.

APP SCAM TYPES

PURCHASE SCAM

ALL PURCHASE SCAM	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 /H1 21 CHANGE
Cases	40,486	43,806	50,327	49,406	53,782	7%
Payments	50,933	56,560	64,948	67,463	72,177	11%
Loss	£23.9m	£27.2m	£32.3m	£31.8m	£31.1m	-4%
Returned to Victim	£6.5m	£8.1m	£9.3m	£11.7m	£16.4m	76%

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 were the most common form of APP scam in the first six months of 2022, with 53,782 cases accounting for 56 per cent of the total number of APP scam cases. A total of £31.1 million was lost to purchase scams during the same period, with most losses being from personal current accounts.

Payment service providers were subsequently able to return £16.4 million of the losses or 53 per cent of the total.

Typically, purchase scams involve lower-value payments, with the smaller average case value meaning that they accounted for only 11 per cent of the total value of APP scams.

Voluntary Code

The figures below relate only to those cases assessed using the voluntary code by signatory PSPs.

All cases reported below cover the period January 2022 to June 2022, are included in previous figures relating to all purchase scam cases reported and should not be treated as an addition.

CODE ONLY: Purchase Scam	Less than £1k	£1k-£10k	More than £10k	Total
Cases	45,073	4,881	241	50,195
Payments	57,731	8,870	885	67,486
Value	£9.2m	£13.2m	£4.8m	£27.3m
Returned to customer	£5.7m	£6.1m	£2.2m	£14.0m

The voluntary code data shows that typically, purchase scams involve lower-value payments (90 per cent of all cases reported totalled less than £1,000) so while purchase scams account for a significant proportion of the case volumes they only account for 14 per cent of the losses.

For only those cases assessed using the code 51 per cent (£14.0 million) of the total was returned to the victim in the first six months of 2022.

How to stay safe from purchase scams:

- Be suspicious of any "too good to be true" offers or prices.
- Use the secure payment method recommended by reputable online retailers and auction sites.
- 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 Credit Consumer Act.
- Read online reviews to check websites and sellers are genuine, and ask to see high value items in person or via video link, as well as getting copies of the relevant documentation to ensure the seller owns the item.
- Purchase items made by a major brand from the list of authorised sellers listed on their official website.
- Always access the website you're purchasing from by typing it into your web browser and be wary of clicking on links in unsolicited emails.
- Always ensure you click 'log out' or 'sign out' of websites.
- If you have visited a website you think is suspicious you can report it to the National Cyber Security Centre.
- Contact your bank straight away if you think you may have fallen for a purchase scam.

INVESTMENT SCAM

ALL INVESTMENT SCAM	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 /H1 21 CHANGE
Cases	3,655	4,526	6,224	5,850	5,166	-17%
Payments	8,720	11,203	17,567	18,098	15,053	-14%
Loss	£47.6m	£61.8m	£90.6m	£81.1m	£61.2m	-32%
Returned to Victim	£14.2m	£22.6m	£34.8m	£37.0m	£31.1m	-11%

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 nearly a third in the first six months of 2022: this may be a result of the decreased amount of opportunities for fraudsters to contact victims now lockdown restrictions have eased. Investment scams still account for the largest value of all eight APP scam types in the first six months of 2022, a continuation of the trend seen in 2020 and 2021 with losses of £61.2 million or 25 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 accounts for five per cent of the total number of APP scam cases.

Payment services providers were subsequently able to return £31.1 million to victims or 51 per cent of the total.

Voluntary Code

The figures below relate only to those cases assessed using the voluntary code by signatory PSPs.

All cases reported below cover the period January 2022 to June 2022, are included in previous figures relating to all investment scam cases reported and should not be treated as an addition.

CODE ONLY: Investment Scam	Less than £1k	£1k-£10k	More than £10k	Total
Cases	2,193	1,403	770	4,366
Payments	3,498	4,101	4,917	12,516
Value	£0.8m	£4.6m	£40.8m	£46.3m
Returned to customer	£0.4m	£2.2m	£23.4m	£26.1m

For only those cases assessed using the code, 56 per cent (£26.1 million) of the total was returned to the victim in the first six months of 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

ROMANCE SCAM

ALL ROMANCE SCAM	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 /H1 21 CHANGE
Cases	1,107	1,218	1,479	1,791	1,662	12%
Payments	6,051	7,134	11,489	14,325	13,907	21%
Loss	£8.5m	£9.3m	£12.7m	£18.2m	£16.6m	31%
Returned to Victim	£2.9m	£3.1m	£4.3m	£7.8m	£8.3m	93%

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 £16.6 million was lost to romance scams in January to June 2022, an increase of 31 per cent when compared to the same period in 2021.

Romance scams have an average of over eight 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 £8.3 million to victims or 50 per cent of the total.

Voluntary Code

The figures below relate only to those cases assessed using the voluntary code by signatory PSPs.

All cases reported below cover the period January 2022 to June 2022, are included in previous figures relating to all romance scam cases reported, and should not be treated as an addition.

CODE ONLY: Romance Scam	Less than £1k	£1k-£10k	More than £10k	Total
Cases	620	609	271	1,500
Payments	1,803	4,459	6,093	12,355
Value	£0.2m	£2.2m	£11.9m	£14.3m
Returned to customer	£0.1m	£1.2m	£6.5m	£7.8m

For only those cases assessed using the code 55 per cent (£7.8 million) of the total was returned to the victim in the first six months of 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.

ADVANCE FEE SCAM

ALL ADVANCE FEE SCAM	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 /H1 21 CHANGE
Cases	5,697	8,136	9,064	11,431	11,540	27%
Payments	9,245	13,987	16,233	20,737	21,017	29%
Loss	£8.3m	£13.9m	£14.1m	£18.1m	£14.6m	4%
Returned to Victim	£3.0m	£4.5m	£5.3m	£6.1m	£6.3m	18%

In an advance fee scam, a criminal convinces their victim to pay a fee which they claim will result in the release of a much larger payment or as a deposit for high-value goods and holidays.

These scams include claims from the criminals that the victim has won an overseas lottery, that gold or jewellery is being held at customs or that an inheritance is due. The fraudster tells the victims that a fee must be paid to release the funds or goods, however, when the payment is made, the promised goods or money never materialise. These scams often begin on social media or with an email, or a letter sent by the criminal to the victim.

Advance fee scams were the third most common form of APP scam in the first half of 2022, accounting for 12 per cent of the total number of cases. A total of £14.6 million was lost to advance fee scams, a four per cent increase on the same period in 2021.

Payment services providers were subsequently able to return £6.3 million to victims or 43 per cent of the total.

Voluntary Code

The figures below relate only to those cases assessed using the voluntary code by signatory PSPs.

All cases reported below cover the period January 2022 to June 2022, are included in previous figures relating to all advance fee scam cases reported, and should not be treated as an addition.

CODE ONLY: Advance Fee Scam	Less than £1k	£1k-£10k	More than £10k	Total
Cases	8,669	2,041	166	10,876
Payments	13,556	4,655	1,630	19,841
Value	£2.2m	£5.0m	£5.9m	£13.1m
Returned to customer	£1.3m	£2.0m	£2.0m	£5.3m

For only those cases assessed using the code 41 per cent (£5.3 million) of the total was returned to the victim in the first six months of 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 must 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 e.g. 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 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.
- Contact your bank straight away if you think you may have fallen for an advance fee scam.

INVOICE AND MANDATE SCAM

ALL INVOICE and MANDATE SCAM	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 /H1 21 CHANGE
Cases	2,778	1,943	2,053	2,277	1,611	-22%
Payments	3,613	2,707	2,813	3,354	2,387	-15%
Loss	£40.1m	£28.6m	£27.1m	£29.6m	£27.1m	0%
Returned to Victim	£16.5m	£13.3m	£10.8m	£11.7m	£15.2m	40%

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.

There has been no change in invoice and mandate scams losses, totalling £27.1 million in both the first six months of 2022 and the first six months of 2021. 67 per cent (£18.2 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 services providers were subsequently able to return £15.2 million to victims or 56 per cent of the total.

Voluntary Code

The figures below relate only to those cases assessed using the voluntary code by signatory PSPs.

All cases reported below cover the period January 2022 to June 2022, are included in previous figures relating to all invoice and mandate scam cases reported and should not be treated as an addition.

CODE ONLY: Invoice & Mandate Scam	Less than £1k	£1k-£10k	More than £10k	Total
Cases	325	669	192	1,186
Payments	405	926	379	1,710
Value	£0.2m	£2.2m	£10.2m	£12.6m
Returned to customer	£0.1m	£1.4m	£6.9m	£8.4m

For only those cases assessed using the code 67 per cent (£8.4 million) of the total was returned to the victim in the first six months of 2022.

How to stay safe from invoice and mandate scams:

- Always confirm any bank account details directly with the company either on the telephone or in person before you make a payment or transfer 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.
- Contact your bank straight away if you think you may have fallen for an invoice or mandate scam.
- 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

ALL CEO SCAM	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 /H1 21 CHANGE
Cases	187	170	230	231	201	-13%
Payments	235	252	331	347	298	-10%
Loss	£2.4m	£2.4m	£6.1m	£6.6m	£7.9m	28%
Returned to Victim	£1.1m	£0.7m	£1.6m	£1.2m	£2.2m	40%

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 was the least common form of APP scam in the first six months of 2022, accounting for less than one per cent of total cases. A total of £7.9 million was lost, equivalent to three per cent of the total case value.

Payment services providers were subsequently able to return £2.2 million to victims or 28 per cent of the total.

Voluntary Code

The figures below relate only to those cases assessed using the voluntary code by signatory PSPs.

All cases reported below cover the period January 2022 to June 2022, are included in previous figures relating to all CEO scam cases reported and should not be treated as an addition.

CODE ONLY: CEO Scam	Less than £1k	£1k-£10k	More than £10k	Total
Cases	6	53	28	87
Payments	7	64	69	140
Value	£3,088	£0.2m	£1.5m	£1.7m
Returned to customer	£2,911	£0.1m	£0.6m	£0.7m

For only those cases assessed using the code 38 per cent (£0.7 million) of the total was returned to the victim in the first six months of 2022.

How to stay safe from CEO fraud:

- 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 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 about any unexpected emails or letters which request urgent bank transfers, even if the message appears to have originated from someone from your own organisation.
- Contact your bank straight away if you think you may have fallen for a CEO fraud.

IMPERSONATION: POLICE / BANK STAFF

ALL IMP: Pol / Bank Staff SCAM	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 /H1 21 CHANGE
Cases	7,983	13,194	17,521	11,885	9,209	-47%
Payments	14,049	26,548	34,774	28,032	22,622	-35%
Loss	£34.7m	£56.1m	£75.6m	£61.8m	£59.6m	-21%
Returned to Victim	£20.0m	£32.1m	£40.6m	£38.6m	£42.2m	4%

In this scam, the criminal contacts the victim purporting to be from either the police or the victim's bank and convinces the victim to make a payment to an account they control.

These scams often begin with a phone call or text message, with the fraudster claiming there has been fraud on the victim's account, and they need to transfer the money to a 'safe account' to protect their funds. However, the criminal controls the recipient account. Criminals may pose as the police and ask the individual to take part in an undercover operation to investigate 'fraudulent' activity at a branch.

To commit this fraud, the criminal will often research their victim first, including using information gathered from other scams and data breaches to make their approach sound genuine.

Police and bank staff impersonation scams accounted for ten per cent of all APP scam cases in the first six months of 2022. £59.6 million was lost due to these scams, which by value was the second highest type of APP scam, accounting for 24 per cent of total losses.

Payment services providers were subsequently able to return £42.2 million to victims or 71 per cent of the total.

Voluntary Code

The figures below relate only to those cases assessed using the voluntary code by signatory PSPs.

All cases reported below cover the period January 2022 to June 2022, are included in previous figures relating to all impersonation: Poilce / Bank staff scam cases reported and should not be treated as an addition.

CODE ONLY: IMP: Pol / Bank Staff Scam	Less than £1k	£1k-£10k	More than £10k	Total
Cases	2,368	5,252	1,155	8,775
Payments	3,818	13,756	4,081	21,655
Value	£1.3m	£20.9m	£33.6m	£55.7m
Returned to customer	£0.9m	£16.0m	£22.5m	£39.4m

For only those cases assessed using the code, 71 per cent (£39.4 million) of the total was returned to the victim in the first six months of 2022.

How to stay safe from impersonation scams:

- Your bank or the police will never ask you to transfer money to a safe account or contact you out of the blue to ask for your full PINs, passwords or passcodes.
- Only give out your personal or financial information to services you have consented to and are expecting to be contacted by.
- Contact your bank or an organisation directly using a known email or phone number.
- Don't give anyone remote access to your computer following a cold call, unsolicited text or email.
- You can forward suspicious-looking emails to report@phishing.gov.uk and suspected scam texts to your mobile network provider by forwarding them to 7726 which spells SPAM on your telephone keypad. 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.
- Contact your bank straight away if you think you may have fallen for a impersonation scam.

IMPERSONATION: OTHER

ALL IMP: OTHER SCAM	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 /H1 21 CHANGE
Cases	7,200	12,528	14,642	11,585	12,048	-18%
Payments	12,223	21,111	24,467	20,159	20,114	-18%
Loss	£22.5m	£33.3m	£43.0m	£34.6m	£30.9m	-28%
Returned to Victim	£10.8m	£15.3m	£19.2m	£17.7m	£18.6m	-3%

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 £30.9 million was lost to this type of scam in H1 2022, a reduction of 28 per cent when compared to the same period in 2021.

Payment services providers were subsequently able to return £18.6 million to victims or 60 per cent of the total.

Voluntary Code

The figures below relate only to those cases assessed using the voluntary code by signatory PSPs.

All cases reported below cover the period January 2022 to June 2022, are included in previous figures relating to all impersonation: other scam cases reported and should not be treated as an addition.

CODE ONLY: IMP: Other Scam	Less than £1k	£1k-£10k	More than £10k	Total
Cases	4,832	5,753	326	10,911
Payments	6,539	10,013	1,508	18,060
Value	£2.3m	£14.6m	£8.6m	£25.6m
Returned to customer	£1.5m	£8.9m	£5.2m	£15.6m

For only those cases assessed using the code 61 per cent (£15.6 million) of the total was returned to the victim in the first six months of 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 such as your name, address, DOB, 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 or unsolicited message.
- Contact your bank straight away if you think you may have fallen for an impersonation scam.

PAYMENT TYPE

These data show the type of payment method the victim used to make the payment in the authorised push payment scam. Faster Payments was used for 98 per cent of fraudulent APP scam payments. While CHAPS was the least common payment method, representing only 0.2 per cent of cases, the high-value nature of transactions using this payment type meant that it accounted for four per cent of the total value

PAYMENT VOLUMES	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 /H1 21 CHANGE
Faster Payment	101,297	135,344	167,720	167,731	164,134	-2%
CHAPS	244	257	435	329	409	-6%
BACS	667	526	729	966	960	32%
Intra Bank Transfer ("on us")	1,402	1,711	2,100	1,258	532	-75%
International	1,459	1,664	1,638	2,231	1,540	-6%
Total	105,069	139,502	172,622	172,515	167,575	-3%

PAYMENT VALUES	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 /H1 21 CHANGE
Faster Payment	£149.3m	£200.1m	£263.7m	£240.8m	£212.2m	-20%
CHAPS	£8.2m	£6.3m	£9.3m	£13.2m	£9.7m	5%
BACS	£15.1m	£8.4m	£11.1m	£9.3m	£13.7m	24%
Intra Bank Transfer ("on us")	£2.7m	£7.9m	£5.3m	£2.3m	£0.5m	-91%
International	£12.9m	£9.9m	£12.2m	£16.2m	£12.9m	6%
Total	£188.1m	£232.6m	£301.5m	£281.8m	£249.1m	-17%

PAYMENT CHANNEL

These data show the channel through which the victim made the authorised push payment. The most common payment channel was mobile banking which accounted for 58 per cent of the payment volume but only 29 per cent of the loss, indicating the typically lower payment limits available to customers within the mobile banking channel.

PAYMENT CHANNEL Volume	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 vs H1 21
Branch	3,445	5,523	4,070	4,181	3,813	-6%
Internet Banking	55,608	58,245	62,789	67,227	63,306	1%
Telephone Banking	2,687	2,906	2,725	3,524	3,214	18%
Mobile Banking	43,329	72,828	103,038	97,583	97,242	-6%
Total	105,069	139,502	172,622	172,515	167,575	-3%

PAYMENT CHANNEL Values	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022	H1 22 vs H1 21
Branch	£19.7m	£23.9m	£27.2m	£29.3m	£25.9m	-5%
Internet Banking	£126.8m	£135.7m	£171.4m	£157.7m	£140.6m	-18%
Telephone Banking	£9.7m	£8.1m	£11.3m	£13.1m	£9.3m	-18%
Mobile Banking	£32.0m	£64.8m	£91.5m	£81.7m	£73.3m	-20%
Total	£188.1m	£232.6m	£301.5m	£281.8m	£249.1m	-17%

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 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.

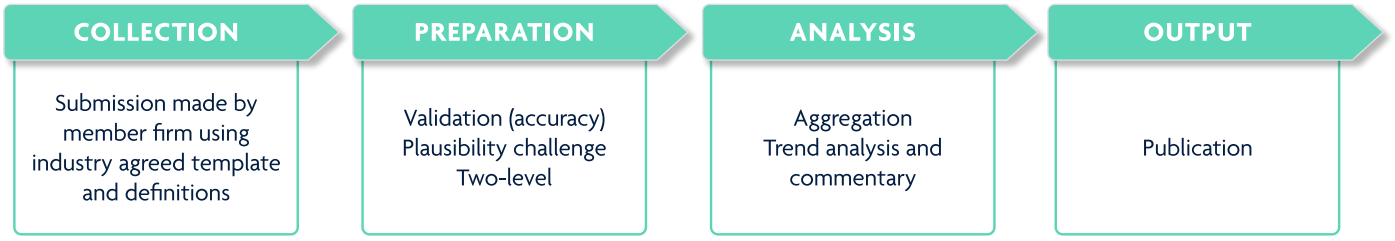
Data plausibility – outputs

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.

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.

A typical process for one submission from one member would look like the below.



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