UK FINANCE

2021 HALF YEAR FRAUD UPDATE

ukfinance.org.uk

INTRODUCTION

The pandemic has seen an evolution in fraud as criminals continuously look for new ways to target potential victims. Latest figures released by UK Finance show the scale of the problem is only growing, despite the efforts of the banking and finance industry.

In the first half of this year, criminals stole a total of £753.9 million through fraud, an increase of over a quarter (30 per cent) compared to H1 2020. The advanced security systems used by banks prevented a further £736 million from being taken.

Over the previous editions, our reports showed the largest fraud losses were due to unauthorised fraud committed using payment cards. However, in the first half of 2021, criminals focused their activity on authorised push payment (APP) fraud, where the customer is tricked into authorising a payment to an account controlled by a criminal.

Using tactics such as scam phone calls, text messages and emails, as well as fake websites and social media posts, criminals seek to trick people into handing over personal details and passwords. This information is then used to target victims and convince them to authorise payments.

APP fraud losses increased 71 per cent during the first half of 2021 - surpassing the amount of money stolen through card fraud for the first time.

There were significant increases in impersonation scams, as criminals posed as banks, government bodies and even health officials to trick people out of their money.

There has also been an increase in purchase scams, where people make a payment for goods they believe to be genuine but which never materialise. Increasingly we are seeing life-changing sums being lost to such scams.

Investment scams are another area of significant concern, 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.

What all these scams have in common is that criminals are using online platforms, including fraudulent advertising through search engines and social media, and fake websites. UK Finance analysis conducted earlier this year found that 70 per cent of authorised push payment scams originated on an online platform.

Worryingly, there has also been a significant increase in online adverts encouraging people to become money mules – where people allow their bank account to be used to 'cash out' fraudulent funds. These adverts 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.

It is difficult to determine how much of the fraud losses are passing through money mule networks, but what is clear is that these money mule accounts enable criminals to get away with fraud, as it is far more difficult for banks to identify such transactions because the money is being passed through existing and legitimate accounts.

The level of fraud in the UK is such that it is now a national security threat. 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.

Throughout the pandemic we have been working with other industries, including mobile phone and network operators and online platforms, to help step up the fight against fraud.

The government's Online Safety Bill presents an important opportunity to ensure greater protection against financial fraud. In May, user-generated content covering crimes such as investment scams and romance scams was added to the list of harms that companies will now have to police in order to protect consumers. However, online advertisements are not covered by the bill, which means that consumers still have little protection against frauds enabled by scam adverts. But while we wait for legislation, the problem of fraud is here, now, and growing, as our latest figures show. So we will continue to work with government, regulators and other sectors, who must all play their part in tackling this truly national problem.

Katy Worobec
Managing Director, Economic Crime
UK Finance

MEASURES TO COMBAT FRAUD

Below we set out some of the measures being undertaken to combat fraud. The banking and finance industry is committed to tackling fraud and scams by:

- Investing in advanced security systems to protect customers from fraud, including real time transaction analysis and behavioural biometrics on devices. The industry prevented £736.1 million of unauthorised fraud in the first six months of 2021, equivalent to £6.49 in every £10 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, jointly chaired by the home secretary and the chancellor. This includes supporting the **Economic Crime Plan**, to harness the combined capabilities of the public and private sectors to make the UK a leader in the global fight against economic crime. We are also working with the government, law enforcement and regulators to develop a more advanced Fraud Action Plan. This will need to include a focus on prevention and tackling money laundering as well as the law enforcement response.
- 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 2020, 2.1 million compromised card numbers were received through our law enforcement strategic partners, and disseminated via the I&I unit to enable card issuers to take the necessary precautions to protect customers.
- Investing in technology such as Mules Insights Tactical Solution (MITS), a technology that helps to track suspicious payments and identify money mule accounts, and Confirmation of Payee, an account name checking service that helps to prevent authorised push payment scams, used when a payment is being made.
- Implementing the APP scams voluntary code, which helps to improve protections, including adding scam warnings during the payment process.
- Delivering customer education campaigns to help prevent consumers being duped by criminals, including the Take Five to Stop Fraud and Don't Be Fooled campaigns. 33 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 scheme allows bank staff 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 £174 million in fraud and led to 934 arrests since launching in 2016.
- 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 the first half of 2021 the Unit prevented an estimated £85 million of fraud, arrested 67 fraudsters and secured 49 convictions.
- Working with the regulator Ofcom to crack down on number spoofing, including the development of a 'do not originate' list. Ofcom has said this work has led to significant successes in preventing criminals from spoofing the phone numbers of trusted organisations.
- Working with text message providers and law enforcement to **block** scam text messages including those exploiting the Covid-19 crisis. 1087 unauthorised sender IDs are currently being blocked to prevent them being used to send scam text messages mimicking trusted organisations, including over 70 related to Covid-19.

To stay safe, customers are urged to follow the advice of the Take Five to Stop Fraud campaign – Stop, Challenge, Protect:

Criminals are experts at impersonating people, organisations and the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment. Stop and think. It could protect you and your money.

Stop: Taking a moment to stop and think before parting with your money or information could keep you safe.

Challenge: Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

Protect: Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

SUMMARY

In this report UK Finance publishes data on losses due to unauthorised fraudulent transactions made using payment cards, remote banking and cheques and authorised push payment (APP) scams.

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

In an authorised push payment scam, the account holder themselves authorises the payment to be made to another account.

The H1 figures show that in the first half of 2021, losses due to unauthorised financial fraud using payment cards, remote banking and cheques rose seven per cent compared to H1 2021, to £398.6 million.

Meanwhile in the first half of 2021, a total of £355.3 million was lost to authorised push payment scams – an increase of 71 per cent compared to losses seen in the same period in 2020.

Drivers of the fraud losses

While the pandemic has seen falls in some types of fraud, others have soared as criminals continue to adapt the methods used to try and trick consumers into handing over account details or personal information that can be used to defraud them of their funds, or finding new ways to access data that can be used to steal from consumers. 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 2021. 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.

There was a significant rise is investment scams, which are heavily enabled by fraudulent advertising, search engines and social media. These are having an increasing impact on the number of cases seen and the associated losses, with members reporting many 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.

The increase in people working from home and the long periods of lockdown have also fuelled an increase in purchase scams, where the victim pays in advance for goods or services that are never received. These scams usually involve the use of an online platform such as an auction website or social media. While some are still Covid-19 related purchase scams, these are not as prevalent as they used to be, although there has been an increase in life changing sums of money being lost.

Fraud losses are also being driven up by the theft of customers' personal and financial data, which often occurs as a result 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.

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.

Since 2018 UK Finance has been reporting enhanced data on overall authorised push payment (APP) scams. Separate data relating to cases under the code was first reported in March 2020.

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.
- Figures reported in previous half-year results may have been amended at end of year due to additional data being presented by members.

UNAUTHORISED FRAUDULENT TRANSACTIONS

January to June 2021 (Cards, Cheques and Remote Banking)

OVERALL	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Prevented Value	£717.6m	£944.7m	£821.7m	£1005.6m	£852.5m	£763.2m	£736.1m	**-14%**	**-4%**
Cases	1,198,130	1,453,426	1,385,486	1,406,825	1,383,352	1,527,157	1,491,656	**8%**	**-2%**
Gross Loss	£400.0m	£444.8m	£408.4m	£416.4m	£374.0m	£409.8m	£398.6m	**7%**	**-3%**

Losses due to unauthorised transactions on cards, cheques and remote banking increased to £398.6 million in the first half of this year, up 7 per cent on the previous year. The number of recorded cases of unauthorised fraudulent transactions rose by 8 per cent to 1.49 million.

There was a fall of 14 per cent in the value of prevented fraud in H1 2021, with banks stopping £736.1 million of attempted unauthorised fraudulent transactions. This equates to the industry preventing £6.49 in every £10 of attempted fraud.

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

AUTHORISED PUSH PAYMENT (APP) SCAMS

January to June 2021

OVERALL AUTHORISED PUSH PAYMENT SCAMS	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Total number of cases	57,549	64,888	66,247	83,699	106,164	**60%**	**27%**
Total case value	£207.5m	£248.3m	£207.8m	£271.2m	£355.3m	**71%**	**31%**
Total returned to the customer	£39.3m	£76.7m	£82.5m	£124.3m	£150.7m	**83%**	**21%**

Total losses due to authorised push payment scams increased to £355.3 million in the first half of 2021, up 71 per cent compared to the same period in 2020. The number of cases rose 60 per cent to 106,164.

While cases of investment scams rose 84 per cent to 6,864, it was impersonation scams – police/bank scam cases – which saw the biggest increase, rising 129 per cent to 18,816.

There has been an increase in the amount returned to victims, from 39 per cent in the first half of 2020, to 42 per cent in the first six months of 2021. 31 per cent of cases were decided in under a week.

UNAUTHORISED DEBIT AND CREDIT AND OTHER PAYMENT CARD FRAUD

OVERALL	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Prevented Value	£501.4m	£625.0m	£489.5m	£518.0m	£486.8m	£496.5m	£489.4m	**1%**	**-1%**
Cases	1,181,533	1,436,206	1,365,112	1,380,427	1,352,646	1,482,976	1,440,739	**7%**	**-3%**
Gross Loss	£305.7m	£365.7m	£313.3m	£307.3m	£287.9m	£286.4m	£261.7m	**-9%**	**-9%**

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 £261.7 million in the first half of 2021, a decrease of 9 per cent on the same period in 2020.

Over this period, overall value of card spending grew by 17 per cent. Card fraud as a proportion of card purchases has decreased from 8.4p in the first half of 2020 to 7.6p in the first half of 2021.

A total of £489.4 million of card fraud was stopped by banks and card companies in the first six months of 2021, an increase of 1 per cent compared to the same period in 2020. This is equivalent to £6.52 in every £10 of attempted card fraud prevented without a loss occurring.

Meanwhile losses from counterfeit card fraud were down 52 per cent compared to the same period a year ago, with the lowest total ever reported.

Contactless losses fell 6 per cent to £7.6 million – the second year in a row we have seen a decrease in contactless losses since we began collecting data. This was due in part to the reduced opportunity for fraudsters to take advantage of contactless during the lockdown period of the pandemic. The value of contactless spending for H1 2021 was £66.5 billion, so losses through contactless remain a tiny proportion of overall transactions.

The finance industry is tackling card fraud by:

- Investing in advanced security systems, including real-time transaction analysis and behavioural biometrics on devices.
- Working with the Financial Conduct Authority (FAC) on the ongoing **phased implementation** of Strong Customer Authentication, new EU-wide rules aimed at reducing fraud by verifying a customer's identify when they make certain higher value online purchases. This was subject to delays because of the Covid-19 pandemic but the deadline for FCA enforcement is March 2022.
- Developing fraud screening detection tools, such as 3D Secure technology which protects card purchases online.
- Fully sponsoring the Dedicated Card and Payment Crime Unit (DCPCU), a specialist police unit which targets organised crime groups responsible for card fraud.

REMOTE PURCHASE FRAUD

OVERALL	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Cases	922,515	1,127,760	1,071,493	1,085,925	1,134,399	1,283,467	1,260,276	**11%**	**-2%**
Gross Loss	£231.8m	£274.6m	£237.4m	£232.8m	£222.8m	£229.8m	£210.5m	**-5%**	**-8%**

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

Losses due to remote purchase fraud decreased by 5 per cent to £210.5 million in the first six months of 2021. The number of cases rose by 11 per cent, resulting in a lower average case value and suggesting 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.

Contained within these figures, e-commerce card fraud totalled an estimated £177 million in the first half of 2021, a reduction of 3 per cent when compared to the same period in 2020.

Staying safe from remote purchase fraud

- 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.
- Do your research before making any purchases and ask to see vehicles in person with the relevant documentation to ensure the seller owns it.
- 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.

LOST AND STOLEN CARD FRAUD

OVERALL	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Cases	204,862	230,129	230,727	229,415	166,710	155,284	144,703	**-13%**	**-7%**
Gross Loss	£45.5m	£49.6m	£48.3m	£46.4m	£41.1m	£37.8m	£35.1m	**-15%**	**-7%**

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 fell by 15 per cent in H1 of this year, compared to the same period last year, down to £35.1 million. The number of incidents also dropped by 13 per cent in H1 2021, compared to H1 2020, resulting in a lower average loss value per case, with bank systems increasingly detecting fraudulent spending on lost or stolen cards more quickly.

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 card company immediately.
- Make sure you fully cover your PIN with your free hand or purse whenever you enter it.
- If you spot anything suspicious with an ATM, or someone is watching you, then do not use the machine and report it to your bank.

CARD NOT RECEIVED FRAUD

OVERALL	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Cases	4,697	5,349	3,949	3,958	4,193	4,242	4,134	**-1%**	**-3%**
Gross Loss	£3.0m	£3.3m	£2.5m	£2.7m	£2.1m	£2.3m	£2.0m	**-4%**	**-13%**

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 fell by 4 per cent the first six months of 2021 to £2 million, while the number of individual cases decreased by just 1 per cent. H1 2021 is the lowest ever recorded total for loss.

Criminals typically target multi-occupancy buildings such as flats to carry out this type of fraud, but greater awareness among consumers of the risks has led to a sharp decrease in card not received fraud. The increased number of people working from home during the pandemic may also have helped to keep this form of fraud down.

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

OVERALL	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Cases	28,109	30,527	30,980	34,927	28,389	24,393	14,782	**-48%**	**-39%**
Gross Loss	£7.9m	£8.4m	£6.6m	£6.2m	£5.4m	£3.3m	£2.6m	**-52%**	**-22%**

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

This information is typically stolen using a device attached to an ATM or unattended payment terminal, such as at a car park. A fake magnetic stripe card is then created and used overseas in countries yet to upgrade to Chip & PIN.

Losses from counterfeit card fraud fell 52 per cent in H1 2021 compared to the same period in 2020, decreasing from £5.4 million to £2.6 million. The number of reported cases fell by 48 per cent. These falls highlight that bank systems are increasingly detecting potentially fraudulent transactions at an earlier stage, and there are fewer opportunities to use cards in non Chip & PIN situations.

How to stay safe from counterfeit card fraud:

- Always protect your PIN by fully covering the keypad with your free hand or purse.
- 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 card company immediately.

CARD ID THEFT

OVERALL	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Cases	21,350	42,441	27,963	26,202	18,955	15,590	16,844	**-11%**	**8%**
Gross Loss	£17.4m	£29.9m	£18.5m	£19.2m	£16.5m	£13.2m	£11.5m	**-30%**	**-13%**

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. The criminal will gather information about the intended victim, often through social engineering, and then contact the card issuer pretending to be the genuine cardholder.

Losses from card ID theft fell 30 per cent in the first six months of 2021 compared to the same period in 2020, from £16.5 million to £11.5 million. The number of individual cases dropped by 11 per cent over the same period. While criminals are using this form of fraud to open accounts in other people's names, earlier detection by banks is helping to drive down losses on a per case basis.

How to stay safe from card ID fraud:

- Don't be tricked into giving a fraudster access to your personal or financial information.
- Never automatically click on a link in an unexpected email or text and always question uninvited approaches.
- Look after your personal documents – keep them secure at home and shred any bills or statements before you throw them away.
- Check your credit record for any applications you don't recognise. You can do this by contacting a credit reference agency.

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 CARD FRAUD

OVERALL	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Gross Loss	£31.4m	£38.4m	£32.4m	£31.9m	£25.5m	£23.3m	£19.5m	**-23%**	**-16%**

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

The majority 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 dropped by 6 per cent in H1 2021 compared to the first half of 2020 – the second year in a row there has been a decrease on contactless spending since we began collecting data. This is due in large part to the lack of opportunities for fraudsters during the lockdown period of the pandemic.

As a proportion of overall spending contactless fraud also remains low, with £7.6 million of losses compared to spending of £66.5 billion over the same period. This equivalent to 1p in every £100 spent using contactless technology being fraudulent.

UK CASH MACHINE FRAUD

OVERALL	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Gross Loss	£15.9m	£16.7m	£15.5m	£14.5m	£15.0m	£13.1m	£12.0m	**-20%**	**-9%**

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 fell by 20 per cent in the first half of 2021, compared to the same period in 2020. While the majority of this fraud is thought to be perpetuated through distraction thefts and card entrapment at ATMs, the decrease in losses suggests a combination of fewer people using cash machines because of lockdowns but also that consumers are becoming more aware of the need to take precautions.

DOMESTIC AND INTERNATIONAL CARD FRAUD

OVERALL	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
UK Fraud	£226.7m	£269.9m	£229.3m	£220.6m	£208.5m	£206.0m	£187.8m	**-10%**	**-9%**
International Fraud	£79.0m	£95.8m	£84.0m	£86.7m	£79.4m	£80.4m	£73.9m	**-7%**	**-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 internationally.

UK card fraud losses fell by 10 per cent to £187.8 million in H1 of this year, compared to the same period in 2020. Meanwhile international fraud losses decreased by 7 per cent, to £73.9 million, in the first six months of this year.

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

UNAUTHORISED REMOTE BANKING FRAUD

OVERALL	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Prevented Value	£141.9m	£175.8m	£129.8m	£139.1m	£181.5m	£212.3m	£225.7m	**24%**	**6%**
Cases	15,915	15,882	18,859	25,061	29,997	43,643	50,537	**68%**	**16%**
Gross Loss	£91.0m	£61.8m	£65.7m	£84.9m	£79.7m	£117.6m	£133.4m	**67%**	**13%**

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 and makes an unauthorised transfer of money from the victims account.

Losses from remote banking fraud rose by 67 per cent in H1 2021, compared to the same period in 2020, from £79.7 million to £133.4 million. Meanwhile the number of cases were up 68 per cent over the same period to 50,537. The increase in both losses and cases of remote banking fraud reflect the growing number of people using remote banking, and a focus by criminals on taking advantage of this. Evidence also suggests that the fraudsters increasingly prefer to target the victims into transferring money themselves.

However, a total of £225.7 million of unauthorised remote banking fraud was prevented in the first six months of 2021, up 24 per cent on the same period in 2020. This is equivalent to £6.29 in every £10 of attempted fraud and demonstrates the value of measures taken by banks to fight fraud.

The finance industry is tackling remote banking fraud by:

- Continuously investing in advanced security systems, including sophisticated ways of authenticating customers, such as using biometrics and customer behaviour analysis.
- Promoting the Take Five to Stop Fraud campaign to educate customers on how they can protect themselves from fraud.
- Sharing intelligence and information on this type of fraud so that security systems can be adapted to stop the latest threats.
- Working with law enforcement, the government, the telecommunications industry and others to further improve security and to identify and prosecute the criminals responsible.

INTERNET BANKING FRAUD

OVERALL	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Cases	11,151	9,753	10,409	15,440	21,312	34,683	41,917	**97%**	**21%**
Gross Loss	£75.6m	£47.4m	£48.8m	£63.1m	£64.3m	£95.4m	£108.9m	**69%**	**14%**

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.

Losses from internet banking rose by 69 per cent in the first six months of 2021, compared to H1 2020, going from £64.3 million to £108.9 million. The number of cases also increased by 97 per cent, to 41,917. Again, these steep rises reflect both the increase in the number of people regularly using internet banking – and a focus by criminals on targeting internet banking customers. £17.7 million (16 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 out of the blue to ask for your PIN or full password. Only give out your personal or financial details to use a service that you have given your consent to, that you trust and that 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 fraudster access to your personal or financial details. Never automatically click on a link in an unexpected email or text.
- Ensure you have the most up-to-date security software installed on your computer, including anti-virus.

TELEPHONE BANKING FRAUD

OVERALL	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Cases	3,464	4,473	5,504	5,695	4,681	2,809	2,319	**-50%**	**-17%**
Gross Loss	£11.4m	£10.6m	£11.6m	£12.0m	£7.9m	£8.1m	£7.3m	**-7%**	**-10%**

Telephone banking fraud occurs when a criminal gains access to a customer's bank account through telephone banking using compromised personal details and passwords and makes an unauthorised transfer of money from it.

Losses due to telephone banking fraud fell by 7 per cent to £7.3 million in the first six months of 2021 and the number of cases fell by 50 per cent to 2,319. This decrease is due in large part to the introduction of voice biometrics which make it harder for criminals to defraud victims and banks. £0.7 million (10 per cent) of these losses across telephone banking 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 or in writing.
- Always question uninvited approaches 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 or even your mother's maiden name), it doesn't mean they are genuine.

MOBILE BANKING FRAUD

OVERALL	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Cases	1,300	1,656	2,946	3,926	4,004	6,151	6,301	**57%**	**2%**
Gross Loss	£4.0m	£3.8m	£5.3m	£9.9m	£7.5m	£14.0m	£17.1m	**127%**	**22%**

Mobile banking fraud occurs when a criminal gains access to a customer's bank account through a banking app downloaded to a mobile device only, using compromised details and passwords. It excludes mobile web browser banking and browser-based banking apps (incidents on these platforms are included in the internet banking fraud figures).

Losses due to mobile banking fraud reached £17.1 million in the first six months of 2021, up 127 per cent per cent compared to the same period in 2020. Meanwhile, the number of recorded cases rose 57 per cent. This rise reflects the growing number of customers using mobile banking – one in two adults now use mobile banking (UK Finance Payment Markets report 2021) – and a larger offering of mobile banking facilities by banks, which has led to mobile banking becoming a renewed focus of attack for fraudsters. £1.9 million (11 per cent) of these losses across mobile banking were recovered after the incident.

How to stay safe from mobile banking fraud:

- Don't be tricked into giving a fraudster access to your personal or security details. Never automatically click on a link in an unexpected email or text 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.

CHEQUE FRAUD

OVERALL	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Prevented Value	£74.3m	£143.9m	£202.3m	£348.5m	£184.2m	£54.3m	£21.0m	**-89%**	**-61%**
Cases	682	1,338	1,515	1,337	709	538	380	**-46%**	**-29%**
Gross Loss	£3.3m	£17.2m	£29.4m	£24.2m	£6.4m	£5.8m	£3.5m	**-45%**	**-40%**

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

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

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

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

Losses from cheque fraud decreased by 45 per cent in the first half of 2021, falling from £6.4 million in H1 2020 to £3.5 million in H1 2021. The number of cases also dropped, by 46 per cent.

The recent fall in cheque fraud has been driven by the reduced use of cheques during the lockdown period as well as increased use of advanced security features on cheques to identify fraudulent ones as they go through the clearing process.

The value of attempted cheque fraud prevented by the banks also fell, by 89 per cent to £21.0 million in the first half of 2021, equivalent to £8.57 of attempted fraud prevented.

How to stay safe from cheque fraud:

- Draw a line through any unused spaces on cheques and complete them using a ballpoint pen or indelible ink.
- Keep your chequebook in a safe location and inform your bank of any missing or lost cheques.
- Wait for cheques to clear before despatching goods or providing services.
- Check bank statements regularly and report any unrecognised transactions to your bank immediately.

AUTHORISED PUSH PAYMENT (APP) SCAMS

UK Finance began collating and publishing data on the losses due to authorised push payments scams (also known as APP scams) in 2017. Since January 2018, UK Finance has collated additional data to provide further analysis of the overall figures. This new data includes the scam type, payment type and payment channel.

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 a range of social engineering tactics to commit this crime. Typically, this includes the criminal posing as genuine individual or organisation and contacting the victim using a range of methods including via the telephone, email and text message. Intelligence suggests that criminals are increasingly using social media to carry out APP scams.

Once the victim has authorised the payment and the money lands in the criminal's account, the criminal will quickly transfer the money out to numerous other accounts, often abroad, where it is then cashed out.

Where a customer authorises the payment themselves, they have no legal protection to cover them for losses – which is different for an unauthorised transaction. However, under the terms of the APP scams voluntary code, where a customer falls victim to an APP fraud, if both the customers and their financial service provider meet the standards set out in the code, and the company is a signatory of the code, then they will be reimbursed.

In January 2018, UK Finance also introduced new Best Practice Standards for banks and building societies responding to APP scam claims. This greatly improved the identification and reporting processes, which has also led to a notable increase in the reported cases of APP fraud.

OVERALL AUTHORISED PUSH PAYMENT SCAMS		H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Personal	Total number of cases	31,510	46,705	53,475	61,256	63,186	80,073	102,058	**62%**	**27%**
	Total number of payments	47,346	67,361	80,440	94,358	98,145	135,723	180,481	**84%**	**33%**
	Total case value	£92.9m	£135.4m	£146.5m	£170.6m	£164.1m	£223.6m	£296.1m	**80%**	**32%**
	Total returned to the customer	£15.4m	£26.9m	£25.6m	£56.6m	£67.6m	£103.2m	£132.2m	**96%**	**28%**
Non - Personal	Total number of cases	2,619	3,790	4,074	3,632	3,061	3,626	4,106	**34%**	**13%**
	Total number of payments	3,618	5,332	5,637	5,014	4,633	7,300	7,107	**53%**	**-3%**
	Total case value	£55.3m	£70.7m	£61.0m	£77.7m	£43.7m	£47.6m	£59.2m	**35%**	**24%**
	Total returned to the customer	£15.5m	£24.8m	£13.6m	£20.1m	£14.9m	£21.1m	£18.4m	**24%**	**-13%**
Total	Total number of cases	34,129	50,495	57,549	64,888	66,247	83,699	106,164	**60%**	**27%**
	Total number of payments	50,964	72,693	86,077	99,372	102,778	143,023	187,588	**83%**	**31%**
	Total case value	£148.2m	£206.1m	£207.5m	£248.3m	£207.8m	£271.2m	£355.3m	**71%**	**31%**
	Total returned to the customer	£30.9m	£51.7m	£39.3m	£76.7m	£82.5m	£124.3m	£150.7m	**83%**	**21%**

Losses due to authorised push payment scams reached £355.3 million in the first half of 2021, a substantial increase of 71 per cent when compared to the same period in 2020. This was split between personal (£296.1 million) and non-personal or business (£59.2 million).

In total there were 106,164 cases of authorised push payment fraud in the first six months of this year alone. Of this total 102,058 were on personal accounts while 4,106 were on non-personal or business cases.

One case can include several payments and there was a total of 187,588 payments during H1 2021.

While the losses recorded as a result of APP scams rose sharply in H1 compared to the previous year, there was also a substantial increase in the funds returned to victims of APP fraud, with financial providers able to return £150.7 million in the first half of 2021, an 83 per cent increase on the sum returned in the same period in 2020.

APP Voluntary Code

On 28 May 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 new 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 also collates and publishes statistics relating to the cases assessed using the voluntary code. This data covers the period 1 January 2021 until 30 June 2021.

This data shows that 95,073 cases have been assessed and closed during H1 2021, with a total value of £248.6 million. Of this, £121.7 million was reimbursed to victims (49 per cent of the total).

Of the 95,073 cases reported, 68 per cent involved values of less than £1,000, while only 6 per cent of cases involved the more life-changing sums of £10,000 plus.

Only those cases assessed using the voluntary code by signatory PSPs

All cases reported below are also included in previous figures relating to all APP cases reported and should not be treated as an addition.

		< £1k	> £1K < £10K	> £10K	TOTAL
VOLUME	Cases	64,717	24,645	5,711	95,073
	Payments	80,832	58,996	21,400	161,228
VALUE	Value	£19.8m	£80.3m	£148.5m	£248.6m
	Reimbursement	£7.1m	£36.5m	£74.0m	£121.7m

The finance industry is tackling authorised push payment scams by:

- Helping to prevent customers being duped by criminals by raising awareness of how to stay safe through the Take Five to Stop Fraud campaign.
- The implementation of an industry code for the reimbursement of victims of authorised push payment scams.
- Implementing standards to ensure those who have fallen victim to fraud or scams get the help they need as quickly as possible.
- Working with government and law enforcement to deter and disrupt criminals and better trace, freeze and return stolen funds, while calling for new powers on information sharing to allow banks to share data to detect and prevent financial crime better.
- Delivering the Banking Protocol – a ground-breaking rapid response scheme through which branch staff can alert police and Trading Standards to suspected frauds taking place. The system is now operational in every police force area and in the first six months of 2021 prevented £32 million of fraud and led to 91 arrests.
- Working with government on making possible legislative changes to account opening procedures to help the industry act more proactively on suspicion of fraud and prevent criminals from accessing financial systems.
- Exploring new ways to track stolen funds moved between multiple bank accounts.

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 & 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 the figures.

PLEASE NOTE: Scam type data was not collected until January 2018.

SCAM TYPES

PURCHASE SCAMS

PURCHASE SCAMS	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Number of cases	21,483	31,138	35,472	37,864	37,516	41,204	52,348	**40%**	**27%**
Number of payments	27,011	39,685	44,252	48,868	47,768	54,834	68,763	**44%**	**25%**
Total value of losses	£19.4m	£26.9m	£27.9m	£31.1m	£27.1m	£30.0m	£37.7m	**39%**	**26%**
Total subsequently returned to the customer	£1.6m	£2.6m	£2.7m	£6.9m	£6.8m	£9.6m	£11.0m	**63%**	**15%**

In a purchase scam, the victim pays in advance for goods or services that are never received. These scams usually involve the use of an online platform such as an auction website or social media. Common scams include the apparent sale of a car or a technology product, such as a phone or computer, advertised at a low price to attract buyers. Criminals also advertise 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.

Purchase scams were a very common form of APP scam, accounting for 49 per cent of the total number of APP scam cases in the first half of 2021. The lower average case value means that they accounted for 11 per cent of the total value of APP scams in the same period.

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

		< £1k	> £1K < £10K	> £10K	TOTAL
VOLUME	Cases	37,261	4,399	772	42,432
	Payments	45,629	11,977	1,520	59,126
VALUE	Value	£9.3m	£11.9m	£5.7m	£26.9m
	Reimbursement	£2.4m	£3.5m	£1.8m	£7.6m

For only those cases which were applicable for assessment using the voluntary code, 28 per cent of all losses were reimbursed to the victim; the smallest proportion across all eight of the scam types. 88 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 'too good to be true' offers or prices.
- Use the secure payment method recommended by reputable online retailers and auction sites.
- Do your research before making any purchases and ask to see the relevant documentation to ensure the seller owns it.
- Purchase items made by a major brand using the list of authorised sellers listed on their official website.
- Always access the website you are purchasing from by typing it into your web browser and be wary of clicking on links in unsolicited emails.

INVESTMENT SCAMS

INVESTMENT SCAMS	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Number of cases	1,359	2,026	3,425	3,364	3,723	5,235	6,864	**84%**	**31%**
Number of payments	3,675	4,261	7,126	7,097	9,492	13,761	20,152	**112%**	**46%**
Total value of losses	£20.8m	£29.3m	£43.4m	£51.9m	£55.2m	£79.9m	£107.7m	**95%**	**35%**
Total subsequently returned to the customer	£1.4m	£2.5m	£2.9m	£9.4m	£15.1m	£33.9m	£44.3m	**193%**	**31%**

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 usually offers high returns to entice their victim. These scams include investment in items such as gold, property, carbon credits, land banks and wine. Increasingly criminals are also targeting victims through the advertisement of fraudulent crypto currency investments, promising people the chance to make vast sums of money quickly.

In the first six months of 2021, losses incurred as a result of investment scams rose by 95 per cent compared to H1 2020, from £55.2 million to £107.7 million. This was equivalent to 30 per cent of the total value of APP scam cases.

Members have reported that investment scams are having an increasing impact on both case volumes and associated losses, as criminals increasingly look to impersonate private banks and investment firms, often setting up cloned websites or social media accounts to draw in unsuspecting consumers. The lack of regulation around social media accounts means this type of fraud is increasingly prevalent and hard to prevent.

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

		< £1k	> £1K < £10K	> £10K	TOTAL
VOLUME	Cases	1,745	1,958	1,592	5,295
	Payments	2,926	5,047	6,142	14,115
VALUE	Value	£0.8m	£7.5m	£66.4m	£74.6m
	Reimbursement	£0.2m	£1.8m	£29.4m	£31.4m

For only those cases which were applicable for assessment using the voluntary code, 42 per cent of all losses were reimbursed to the victim; in the six months before the code was introduced (Jan to June 2019) only 7 per cent of losses were refunded.

How to stay safe from investment scams:

- Be cautious of unsolicited approaches presenting you with exclusive investment opportunities.
- It could be a scam if you are being pressurised to act quickly.
- Check the Financial Conduct Authority's register for regulated firms, individuals and bodies. You can check if a website is genuine by checking their web address.

ROMANCE SCAMS

ROMANCE SCAMS	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Number of cases	571	833	935	1,228	1,291	1,693	1,624	**26%**	**-4%**
Number of payments	3,372	4,202	4,388	6,629	6,170	8,702	14,005	**127%**	**61%**
Total value of losses	£5.3m	£7.3m	£7.9m	£10.2m	£9.3m	£11.9m	£15.1m	**62%**	**27%**
Total subsequently returned to the customer	£0.3m	£0.3m	£0.5m	£1.8m	£2.8m	£5.3m	£5.3m	**88%**	**0%**

In a romance scam, the victim is convinced to make a payment to a person they have only met remotely, often online through social media or dating websites, and with whom they believe they are in a relationship . The 'relationship' is often developed over a long period and the individual is convinced to make multiple, generally smaller, payments to the criminal.

Romance scams accounted for less than 2 per cent of the total number of APP scam cases in the first six months of 2021 and just 4 per cent of the total value.

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

		< £1k	> £1K < £10K	> £10K	TOTAL
VOLUME	Cases	1,218	605	242	2,065
	Payments	1,903	5,482	3,611	10,996
VALUE	Value	£0.2m	£2.3m	£8.4m	£10.9m
	Reimbursement	£0.1m	£0.9m	£3.3m	£4.3m

For only those cases which were applicable for assessment using the voluntary code, 39 per cent of all losses were refunded to the victim; in the six months before the code was introduced (Jan to June 2019) only 6 per cent was returned.

How to stay safe from romance scams:

- Avoid sending money to someone you have never met in person.
- Research the person you are talking to as profile photos may not be genuine.
- 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 any meetings in person take place in public.
- Always consider the possibility of a scam.
- Only accept friend requests from people you know and trust.

ADVANCE FEE SCAMS

ADVANCE FEE SCAMS	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Number of cases	3,646	4,487	4,601	6,110	5,680	8,448	9,840	**73%**	**16%**
Number of payments	6,045	7,226	7,345	9,759	9,343	14,683	17,786	**90%**	**21%**
Total value of losses	£5.9m	£8.0m	£8.2m	£9.1m	£8.0m	£15.1m	£16.8m	**110%**	**11%**
Total subsequently returned to the customer	£0.5m	£0.9m	£0.7m	£1.6m	£2.3m	£5.7m	£5.5m	**135%**	**-3%**

In an advance fee scam, a criminal convinces their victim to pay an upfront fee which they claim would result in the release of a much larger payment or high-value goods – however, no such payment or goods exist. These scams include the criminal claiming that the victim has won an overseas lottery or that gold or jewellery is being held at customs and a fee must be paid to release the funds or goods.

Advance fee scams were the fourth most common form of APP scam in the first half of 2021, accounting for 9 per cent of the total number of cases. However, by value these scams accounted for five per cent.

Only those cases assessed using the voluntary code by signatory PSPs
All cases reported below are also included in previous figures relating to all advance fee scam cases reported and should not be treated as an addition.

		< £1k	> £1K < £10K	> £10K	TOTAL
VOLUME	Cases	6,075	1,586	248	7,909
	Payments	8,726	3,796	1,049	13,571
VALUE	Value	£1.9m	£4.1m	£6.1m	£12.1m
	Reimbursement	£0.6m	£1.1m	£1.9m	£3.6m

For only those cases which were applicable for assessment using the voluntary code, 29 per cent of all losses were refunded to the victim; in the six months before the code was introduced (Jan to June 2019) only 8 per cent was returned.

How to stay safe from advance fee scams:

- Question claims that you are due money for goods or services that you have not ordered or were unaware of, especially if you have to pay any fees upfront.
- It's extremely unlikely that you have won a competition or lottery that you have not 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 e.g. Yahoo, Hotmail or Gmail.
- Confirm organisations you're being contacted by are registered at Companies House and use the details provided to contact recruitment companies and other organisations directly. You can ensure 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.

INVOICE AND MANDATE SCAMS

INVOICE & MANDATE SCAMS	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Number of cases	2,857	4,697	4,659	3,913	2,849	2,106	2,166	**-24%**	**3%**
Number of payments	3,703	6,195	6,052	5,416	3,919	3,177	3,159	**-19%**	**-1%**
Total value of losses	£52.1m	£71.7m	£55.9m	£58.2m	£45.6m	£36.3m	£42.2m	**-7%**	**16%**
Total subsequently returned to the customer	£13.2m	£23.2m	£13.5m	£18.8m	£19.6m	£17.7m	£13.1m	**-33%**	**-26%**

In an invoice or mandate scam, the victim attempts to pay an invoice to a legitimate payee, but the scammer intervenes to convince the victim to redirect the payment to the scammer's account. This type of fraud often involves email interception or compromise. 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.

The majority of losses by value were from non-personal or business accounts at £26.5million, compared to £15.7 million of losses seen against personal accounts. Typically, corporate invoices will be larger than personal invoices and therefore more attractive a target for fraudsters.

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

		< £1k	> £1K < £10K	> £10K	TOTAL
VOLUME	Cases	440	813	322	1,575
	Payments	524	1,196	718	2,438
VALUE	Value	£0.2m	£2.9m	£12.4m	£15.5m
	Reimbursement	£0.1m	£1.3m	£8.2m	£9.6m

For only those cases which were applicable for assessment using the voluntary code, 62 per cent of all losses were returned to the victim; in the six months before the code was introduced (Jan to June 2019) only 24 per cent was refunded.

How to stay safe from invoice and mandate scams:

- Confirm service provider bank account details directly with the company before payment is made.
- When paying someone for the first time, transfer a small amount first and check payment has been received directly by the company.
- Where possible, send confirmation of payment to service providers once their invoice has been paid

CEO FRAUD

CEO	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Number of cases	347	256	340	336	241	596	207	**-14%**	**-65%**
Number of payments	478	353	487	475	361	770	310	**-14%**	**-60%**
Total value of losses	£8.0m	£6.8m	£7.9m	£9.8m	£4.7m	£5.7m	£6.5m	**37%**	**14%**
Total subsequently returned to the customer	£2.2m	£2.1m	£2.1m	£1.7m	£2.2m	£1.7m	£3.0m	**36%**	**72%**

CEO fraud is where a victim attempts to make a payment to a legitimate payee, but the scammer manages to intervene by impersonating the CEO or other senior person of the victim's organisation to convince them to redirect the payment to the scammer's account. This type of fraud mostly affects businesses. 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 with a request to change payment details or make an urgent payment to a new account.

CEO fraud was the least common form of APP scam in the first half of 2021, accounting for 207 cases – less than 1 per cent of total cases. It accounted for two per cent of total losses.

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

		< £1k	> £1K < £10K	> £10K	TOTAL
VOLUME	Cases	12	45	41	98
	Payments	21	50	63	134
VALUE	Value	£0.0m	£0.3m	£1.2m	£1.5m
	Reimbursement	£0.0m	£0.2m	£0.8m	£1.0m

For only those cases which were applicable for assessment using the voluntary code, 66 per cent of all losses were returned to the victim; the same as the six months before the code was introduced (Jan to June 2019).

How to stay safe from CEO fraud:

- Confirm urgent payment requests, either in person or over the phone, using a known telephone number or by a known email address.
- Be wary of unexpected emails or letters requesting urgent payment, even if it appears to be from someone in your own business.
- Be careful with the type of information you share online about your business.
- Educate employees on CEO scams and update them on the latest threats.
- Ensure employees feel comfortable approaching senior staff to verify payment requests and are aware of the types of requests they should be expecting.
- Make sure all staff check for irregularities before processing payments and changing bank details.

IMPERSONATION: POLICE/BANK STAFF

IMPERSONATION: POLICE/ BANK	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Number of cases	1,947	3,512	4,242	6,846	8,222	13,245	18,816	**129%**	**42%**
Number of payments	3,196	5,507	10,056	12,204	14,478	27,510	39,246	**171%**	**43%**
Total value of losses	£22.2m	£34.3m	£35.4m	£48.7m	£36.7m	£59.9m	£84.7m	**131%**	**41%**
Total subsequently returned to the customer	£6.9m	£12.9m	£11.2m	£26.1m	£23.4m	£36.1m	£48.7m	**108%**	**35%**

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. Often the fraudster will claim 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 actually 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.

Police/bank staff impersonation scams accounted for 18 per cent of all APP scam cases in the first half of 2021. However, by value this scam was the second highest, accounting for 24 per cent of total losses. This highlights the need for the police to also promote the fraud awareness messaging.

Only those cases assessed using the voluntary code by signatory PSPs
All cases reported below are also included in previous figures relating to all Impersonation: Police/Bank scam cases reported and should not be treated as an addition.

		< £1k	> £1K < £10K	> £10K	TOTAL
VOLUME	Cases	4,421	10,044	1,690	16,155
	Payments	6,118	21,588	5,775	33,481
VALUE	Value	£2.6m	£35.4m	£33.9m	£71.9m
	Reimbursement	£1.4m	£21.0m	£21.3m	£43.6m

For only those cases which were applicable for assessment using the voluntary code, 61 per cent of all losses were refunded to the victim; the highest of all eight scam types, in the six months before the code was introduced (Jan to June 2019) only 26 per cent was refunded.

How to stay safe from impersonation scams:

- Never disclose your PIN or let anyone persuade you to hand over your bank card, financial information or withdraw cash.
- Don't feel pressured. Don't agree to hand over money at the door. Take time to think about it and talk to someone you trust.
- Only let someone in if you're expecting them or if they're a trusted friend, family member or professional. Don't feel embarrassed about turning someone away.
- Check their credentials. You should always check someone's credentials – a genuine person won't mind. You can phone the company they represent or check online but never use the contact details they give you.
- Take the time to think about any offer, even if it is genuine. Don't be embarrassed to say 'No' or ask them to leave.

IMPERSONATION: OTHER

IMPERSONATION: OTHER	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Number of cases	1,919	3,546	3,875	5,227	6,725	11,172	14,299	**113%**	**28%**
Number of payments	3,484	5,264	6,371	8,924	11,247	19,586	24,167	**115%**	**23%**
Total value of losses	£14.4m	£21.8m	£20.9m	£29.3m	£21.2m	£32.5m	£44.7m	**111%**	**37%**
Total subsequently returned to the customer	£4.9m	£7.0m	£5.5m	£10.4m	£10.2m	£14.4m	£19.8m	**93%**	**37%**

In this scam, a criminal typically contacts the victim purporting to be from an organisation other than the police or the victim's bank and asks the victim to make a payment. Fraudsters often pose as organisations such as utility companies, communications service providers or government departments and claim that the victim must settle a fictitious fine or return an erroneous refund. The scams can often involve the criminal requesting remote access to the victim's computer.

13 per cent of all APP scam cases were due to this type of scam in the first half of 2021, accounting for 13 per cent of total losses.

Only those cases assessed using the voluntary code by signatory PSPs
All cases reported below are also included in previous figures relating to all Impersonation: Other scam cases reported and should not be treated as an addition.

		< £1k	> £1K < £10K	> £10K	TOTAL
VOLUME	Cases	5,948	5,195	804	11,947
	Payments	7,388	9,860	2,522	19,770
VALUE	Value	£3.4m	£16.1m	£14.5m	£33.9m
	Reimbursement	£1.0m	£6.8m	£7.4m	£15.2m

For only those cases which were applicable for assessment using the voluntary code, 45 per cent of all losses were refunded to the victim. In the six months before the code was introduced (Jan to June 2019) only 26 per cent was refunded.

How to stay safe from impersonation scams:

- Always question uninvited approaches in case it's a scam. Instead, contact the company directly using a known email or phone number.
- Fraudsters may have some details about you, 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 victim to an impersonation scam.

PAYMENT TYPE

PAYMENT TYPE	VOLUME								
	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Faster Payment	47,515	67,817	81,629	94,187	97,939	137,067	183,821	**88%**	**34%**
CHAPS	357	295	657	683	1,214	816	385	**-68%**	**-53%**
BACS	597	857	1,052	1,276	466	401	604	**30%**	**51%**
Intra Bank transfer	921	801	612	1353	650	945	1,429	**120%**	**51%**
International	1,574	2,923	2,127	1,873	2,509	3,794	1,349	**-46%**	**-64%**
Total	**50,964**	**72,693**	**86,077**	**99,372**	**102,778**	**143,023**	**187,588**	**83%**	**31%**

PAYMENT TYPE	VALUE								
	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Faster Payment	£99.4m	£152.3m	£155.3m	£178.1m	£163.5m	£234.7m	£325.7m	**99%**	**39%**
CHAPS	£13.3m	£12.7m	£10.2m	£19.8m	£11.8m	£8.8m	£8.3m	**-30%**	**-6%**
BACS	£9.5m	£14.1m	£13.2m	£18.3m	£13.8m	£7.2m	£9.2m	**-33%**	**27%**
Intra Bank transfer	£2.0m	£1.3m	£1.0m	£2.6m	£0.8m	£5.6m	£2.2m	**187%**	**-61%**
International	£24.0m	£25.9m	£27.9m	£29.5m	£18.1m	£15.0m	£10.0m	**-45%**	**-33%**
Total	**£148.2m**	**£206.1m**	**£207.5m**	**£248.3m**	**£207.8m**	**£271.2m**	**£355.3m**	**71%**	**31%**

This data shows the type of payment method the victim used to make the authorised push payment. Faster Payment was used in 98 per cent of cases and accounted for 92 per cent of losses by value.

PAYMENT CHANNEL

PAYMENT CHANNEL	VOLUME								
	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Branch	3,344	4,575	6,533	4,539	3,335	5,310	3,768	**13%**	**-29%**
Internet Banking	39,155	54,311	58,147	61,077	53,566	58,644	70,916	**32%**	**21%**
Telephone Banking	2,278	2,243	2,248	3,753	2,775	5,964	6,739	**143%**	**13%**
Mobile Banking	6,187	11,564	19,149	30,003	43,102	73,105	106,165	**146%**	**45%**
Total	**50,964**	**72,693**	**86,077**	**99,372**	**102,778**	**143,023**	**187,588**	**83%**	**31%**

PAYMENT CHANNEL	VALUE								
	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	H2 2020	H1 2021	H1 vs H1 CHANGE	H1 vs H2 CHANGE
Branch	£18.9m	£22.3m	£24.2m	£24.9m	£20.3m	£24.7m	£26.4m	**30%**	**7%**
Internet Banking	£120.0m	£168.6m	£158.6m	£186.1m	£146.3m	£170.0m	£219.0m	**50%**	**29%**
Telephone Banking	£6.1m	£8.7m	£12.0m	£15.5m	£13.1m	£15.4m	£16.3m	**24%**	**6%**
Mobile Banking	£3.1m	£6.4m	£12.7m	£21.8m	£28.1m	£61.1m	£93.6m	**233%**	**53%**
Total	**£148.2m**	**£206.1m**	**£207.5m**	**£248.3m**	**£207.8m**	**£271.2m**	**£355.3m**	**71%**	**31%**

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

UK Finance is urging customers to follow the advice of the **Take Five to Stop Fraud** campaign.

Criminals are experts at impersonating people, organisations and the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment. Stop and think: it could protect you and your money.

Always follow the advice of the Take Five to Stop Fraud campaign and Stop, Challenge, Protect when being asked for your money or information.

www.takefive-stopfraud.org.uk

- **Stop:** Taking a moment to stop and think before parting with your money or information could keep you safe.
- **Challenge:** Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Protect:** Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

If you have any questions about this report, please contact the press team:
press@ukfinance.org.uk

For general information about payments and UK Finance please contact:
info@ukfinance.org.uk