UK FINANCE

2020 HALF YEAR FRAUD UPDATE

ukfinance.org.uk

INTRODUCTION

Whether it's elaborate scams and attempts by criminals to con innocent victims into handing over their money or providing access to data which can then be used to gain illicit funds, stories of those impacted by fraud are becoming increasingly common. In particular, Covid-19 has seen criminal gangs focus on taking advantage of people's fears and uncertainties around the virus, sometimes to devastating effect.

This is demonstrated by a sharp rise in the number of impersonation scams, which nearly doubled in the first six months of the year, with almost 15,000 cases reported. Such scams occur when the victim is convinced to make a payment to a criminal claiming to be from a trusted organisation such as the police, a bank or a government department. In some notable cases recently, fraudsters have tricked victims by pretending to offer government grants to help with Covid-19.

Fraudsters have also changed tactics towards more online scams, such as fake investments promoted on search engines, fake goods such as hot tubs listed on auction websites and criminals posing as would-be partners on online dating platforms. In the first half of 2020, a total of £207.8 million was lost to authorised push payment (APP) fraud. Losses to unauthorised fraud in contrast fell by eight per cent in the first half of this year to £374.3 million, with the banking and finance industry preventing £853 million of attempted unauthorised fraud. This was equivalent to losses seen in the same period in 2019.

The voluntary code on APP fraud, introduced in May 2019, has meant more customers are now being reimbursed, particularly for more sophisticated scams involving life-changing sums of money. £73.1 million of APP fraud losses were returned to victims, up 86 per cent compared to the same period last year.

We know from experience that there is often a delay between criminals obtaining people's details and using them to commit fraud, meaning the full losses from Covid-19 related scams designed to harvest people's data are likely to not yet have been fully realised. So it is important that we all follow the advice of the **Take Five to Stop Fraud** campaign and always take a moment to stop and think before parting with money or information in case it's a scam.

The finance industry is working hard to tackle fraud but it is vital that government, regulators, and other sectors continue to step up and play their part in detecting and preventing this criminal activity. In particular, vulnerabilities exploited by fraudsters which are outside the control of the banking industry need to be addressed. Online platforms which allow fraudsters to advertise, services which allow fraudsters to 'spoof' phone numbers to fool the victim and companies who allow their customer data to be accessed all need to play their part in fighting fraud and protecting consumers.

A new regulatory framework is urgently needed to address vulnerabilities in other sectors. We are calling for fraud to be included in the scope of the government's new online harms regulatory framework, to help ensure that online platforms address vulnerabilities that are being exploited by criminals to commit fraud. Fraud shows no sign of easing. It's vital that everyone works together to tackle this scourge, to ensure that the criminal is not the only winner.

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 finance industry is committed to tackling fraud and scams by:

- 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 has prevented £116 million of fraud and led to 744 arrests since it began being rolled out in 2016.
- Investing in advanced security systems to protect customers, including real-time transaction analysis, behavioural biometrics on devices and technology to identify the different sound tones that every phone has and the environment that they are in.
- Working with text message providers and law enforcement to block scam text messages including those exploiting the Covid-19 crisis. 821 unauthorised sender IDs are currently being blocked to prevent them being used to send scam text messages mimicking trusted organisations, including 70 related to Covid-19.
- Working with the regulator Ofcom to crack down on number spoofing, including through 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. For example, when HMRC added numbers to this list they reported reducing "to zero the number of phone scams spoofing genuine inbound HMRC numbers."
- Working closely with the government and law enforcement to tackle fraud through a national Economic Crime Plan, including regularly exchanging information and coordinating responses to emerging threats such as scams linked to Covid-19.
- Helping customers stay safe from fraud and spot the signs of a scam through the Take Five to Stop Fraud campaign. 27 major banks and buildings societies have signed up to the new Take Five Charter, bringing the industry together to give people simple and consistent fraud awareness advice.
- Sponsoring a specialist police unit, the Dedicated Card and Payment Crime Unit (DCPCU), which tackles the organised criminal groups (OCGs) responsible for financial fraud and scams. In the first half of 2020, the unit prevented an estimated £12.5 million of fraud, secured 30 convictions and disrupted seven OCGs.
- Introducing a voluntary code to better protect customers and reduce the occurrence of authorised push payment (APP) fraud. The code became effective for signatory firms on 28 May 2019.
- Working with Pay.UK to implement Confirmation of Payee, an account name checking service that helps prevent authorised push payment scams. Since 30 June 2020 the measure has been fully implemented by the UK's six largest banking groups, covering around 90 per cent of bank transfers.
- Working with Pay.UK to implement the Mule Insights Tactical Solution (MITS), a new technology that will help track suspicious payments and identify money mule accounts.

- Working with the Financial Conduct Authority on the 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.

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 2020, losses due to unauthorised financial fraud using payment cards, remote banking and cheques decreased eight per cent, to £374.3 million.

Meanwhile in the first half of 2020, a total of £207.8 million was lost to authorised push payment scams. This was equivalent to losses seen in the same period in 2019.

From next year we will be comparing the H1 figures to H2 from the previous year, in order to identify and portray a more accurate and timely picture of fraud trends.

UNAUTHORISED FRAUDULENT TRANSACTIONS:

January to June 2020 (Cards, Cheques and Remote Banking)

OVERALL	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	CHANGE
Prevented Value	£678.7m	£708.9m	£751.4m	£706.8m	£717.6m	£944.7m	£820.2m	£1005.6m	£852.9m	**4%**
Cases	937,274	920,232	936,699	973,308	1,198,130	1,453,426	1,385,447	1,406,825	1,397,420	**1%**
Gross Loss	£400.4m	£368.4m	£365.8m	£365.5m	£400.0m	£444.8m	£408.3m	£464.8m	£374.3m	**-8%**

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

Losses due to unauthorised transactions on cards, cheques and remote banking dropped to £374.3 million in the first half of this year, down by eight per cent on the previous year. The number of recorded cases of unauthorised fraudulent transactions rose by one per cent to 1.4 million.

There was a four per cent increase in prevented fraud in H1 2020, with banks stopping £852.9 million of attempted unauthorised fraudulent transactions. This equates to the industry preventing £6.95 in every £10 of attempted fraud.

AUTHORISED PUSH PAYMENT (APP) SCAMS:

January to June 2020

OVERALL AUTHORISED PUSH PAYMENT SCAMS	H1 2019	H2 2019	H1 2020	CHANGE
Total number of cases	57,549	64,888	66,247	**15%**
Total case value	£207.5m	£248.3m	£207.8m	**0%**
Total returned to the customer	£39.3m	£76.7m	£73.1m	**86%**
Total number of payments	86,077	99,372	102,778	**19%**

Total losses due to authorised push payment scams were £207.8 million in the first half of 2020, static compared to the same period in 2019. The number of cases rose 15 per cent to 66,247.

Purchase scams form the highest volume of APP scams and rose by six percent to 37,516, but it was impersonation scams – police/bank scam cases – which saw the biggest increase, rising 94 per cent to 8,222.

There has been an increase in the amount returned to victims, from 19 per cent in the first half of 2019, to 35 per cent in the first six months of 2020, following the introduction of the APP code in May of last year. 40 per cent of cases are now decided in under a week. This covers all cases and not just those under the APP code.

The impact of Covid-19 on fraud levels and the industry's response

Criminals are constantly adapting the methods used to try and trick consumers into handing over their money or personal information. Since the pandemic began, we have seen how quickly they have adapted to and exploited Covid-19 with a growth in fraud and scams that target people online. These include fake goods listed on auction websites, criminals posing as would-be partners on online dating platforms and money mules recruited on social media.

Social engineering, in which criminals groom and manipulate people into divulging personal or financial details or transferring money, was a key driver of both unauthorised and authorised fraud losses in the first half of 2020. A common form of social engineering is an impersonation scam, where a fraudster contacts a customer by phone, text message, email or social media pretending to be a genuine organisation, such as a bank, the police, a utility company or a government department. They will typically then persuade the unsuspecting victim to transfer funds or make a payment, or hand over personal information, in the belief they are dealing with a genuine trusted organisation. Intelligence reported to UK Finance suggests that the rise in social engineering scams is being driven in part by criminals exploiting Covid-19. These scams include fraudsters sending emails or text messages pretending to be from government departments and offering grants related to Covid-19. Criminals may also get in touch claiming to be from an airline or travel agency, offering refunds for flights or holidays that have been cancelled due to the pandemic. Additionally, criminals are exploiting the growing numbers of people working remotely, by posing as IT departments or software

providers and claiming that payments are needed to fix problems with people's internet connection or broadband. There is sometimes a delay between criminals obtaining people's details through these scams and using them to commit fraud. This means the full losses from Covid-19 related social engineering scams in the first half of this year are likely to not yet have been fully realised.

Another area where we have a seen a significant rise in losses is investment scams. Here again, intelligence suggests that criminals are increasingly using online platforms to target their victims and are using ever more sophisticated techniques. This includes adverts on search engines or social media platforms, which tend to take the unsuspecting investor to a cloned website impersonating an FCA-regulated firm. Customers will then often be instructed to complete online forms to register their interest, before receiving a call from someone impersonating a genuine investment firm or broker. Purchase scams have also seen a steady rise, as criminals continue to exploit demand for specific items linked to the current pandemic, including bogus pet sales and Personal Protective Equipment and home testing kits. Fictional goods such as fashion items, games consoles and vehicles also continue to be advertised on social media platforms and auction sites.

The Dedicated Card and Payment Crime Unit (DCPCU), the specialist police unit funded by the banking and finance industry, has seen a rise in cases of criminals using the Covid-19 outbreak to defraud vulnerable members of the public. The unit executed 25 warrants between March and June 2020 in enforcement activity against individuals seeking to use Covid-19 as an opportunity to target victim. In one case, the unit successfully prosecuted a criminal in London responsible for sending out thousands of scam text messages claiming to be from the UK government or mobile phone operators. The DCPCU has also worked in partnership with several social media platforms to identify accounts that featured posts relating to payment crime, with over 575 social media accounts linked to fraudulent activity taken down in the first half of this year.

The banking and finance sector has also been working closely with the mobile industry and the National Cyber Security Centre (NCSC) to prevent criminals from sending scam text messages exploiting the Covid-19 crisis. As part of a cross-industry initiative, a block list has been established to block messages from sender IDs that have been used to send scam texts. 821 unauthorised sender IDs are currently being blocked to prevent them being used to send scam text messages mimicking trusted organisations, including 70 related to Covid-19. The industry is also working with the regulator Ofcom to crack down on number spoofing, including through 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. For example, when HMRC added numbers to this list they reported reducing "to zero the number of phone scams spoofing genuine inbound HMRC numbers."

In addition, through the Take Five to Stop Fraud campaign, UK Finance has been regularly promoting advice to help consumers and businesses stay safe from scams related to Covid-19. This has included highlighting the top ten Covid-19 scams the public should be aware of, a warning about holiday scams such as refund offers and fake caravan listings, and advice on how criminals are using the pandemic to impersonate trusted organisations. The Take Five to Stop Fraud campaign has published a **toolkit** to help businesses stay safe from scams. 27 major banks and buildings societies have signed up to the Take Five Charter, bringing signatories together to deliver consistent and concerted fraud awareness and advice.

We expect that criminals will continue to adapt and exploit the impact of coronavirus as we move onto the next stage in this crisis. This could include more social engineering scams exploiting people's financial insecurities by offering payments related to the pandemic, purchase scams offering bogus products at discounted prices on auction websites and social media posts aimed at recruiting money mules who are looking to make quick and easy money. The banking and finance industry will keep taking action on every front to protect customers from this threat, while calling for a stronger regulatory framework that ensures online platforms and other sectors play their part in tackling fraud.

Our fraud data

UK Finance publishes both the value of fraud losses and the number of cases. The data is reported to us by our members which include financial providers, credit, debit and charge card issuers, and card payment acquirers.

Each incident of fraud does not equal one person being defrauded, but instead refers to the number of cards or accounts defrauded. For example, if a fraud was carried out on two cards, but they both belonged to the same person, this would represent two instances of fraud, not one.

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

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 of this year.

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 DEBIT AND CREDIT AND OTHER PAYMENT CARD FRAUD

OVERALL	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	CHANGE
Prevented Value	£475.7m	£510.3m	£502.4m	£482.4m	£501.4m	£625.0m	£488.2m	£518.0m	£487.2m	**0%**
Cases	917,479	903,247	916,867	956,649	1,181,533	1,436,206	1,365,112	1,380,427	1,366,714	**0%**
Gross Loss	£321.5m	£296.5m	£286.7m	£278.8m	£305.7m	£365.7m	£313.3m	£355.7m	£288.2m	**-8%**

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 £288.2 million in the first half of 2020, a decrease of eight per cent on the same period in 2019.

Over this period, overall value of card spending fell by eight per cent. Card fraud as a proportion of card purchases has remained at 8.4p per £100 spent in the first half of 2020.

A total of £487.2 million of card fraud was stopped by banks and card companies in the first six months of 2020, which represents no change compared to the same period in 2019. This is equivalent to £6.28 in every £10 of attempted card fraud prevented without a loss occurring.

Meanwhile losses from counterfeit card fraud were down 12 per cent compared to the first same period a year ago, the lowest total ever reported.

Contactless losses fell 20 per cent to £8.2 million, the first time 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 2020 was £41 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 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 has been subject to delays because of the Covid-19 pandemic.
- Developing fraud screening detection tools, such as 3D Secure technology which protects card purchases online.
- Working with government and law enforcement in the Joint Fraud Taskforce to use our collective powers, systems and resources to crack down on financial fraud.
- Fully sponsoring the Dedicated Card and Payment Crime Unit (DCPCU), a specialist police unit which targets organised crime groups responsible for card and payment fraud.

REMOTE PURCHASE FRAUD

OVERALL	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	CHANGE
Cases	728,087	709,745	703,729	694,424	922,515	1,127,760	1,071,493	1,085,925	1,124,671	**5%**
Gross Loss	£224.1m	£208.2m	£204.8m	£203.6m	£231.8m	£274.6m	£237.4m	£268.7m	£222.0m	**-6%**

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 6 per cent to £222 million in the first six months of 2020.

The number of cases rose by five 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 £183 million in the first half of 2020, static when compared to the same period in 2019.

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 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	CHANGE
Cases	109,110	122,054	148,474	201,805	204,862	230,129	230,727	229,415	187,054	**-19%**
Gross Loss	£49.5m	£46.8m	£47.8m	£45.1m	£45.5m	£49.6m	£48.3m	£54.0m	£42.6m	**-12%**

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 12 per cent in H1 of this year, compared to the same period last year, reaching £42.6 million. The number of incidents also dropped by 19 per cent in H1 2020 compared to H1 2019, 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 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, purse or wallet 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 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	CHANGE
Cases	5,685	5,692	5,466	5,437	4,697	5,349	3,949	3,958	3,440	**-13%**
Gross Loss	£6.1m	£6.4m	£5.6m	£4.6m	£3.0m	£3.3m	£2.5m	£3.1m	£2.0m	**-20%**

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 fell by 20 per cent in the first six months of 2020 to £2 million, with the number of individual cases also dropping by 13 per cent. This represented the lowest ever recorded total. 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.

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 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	CHANGE
Cases	58,268	50,329	43,426	41,599	28,109	30,527	30,980	34,927	30,441	**-2%**
Gross Loss	£21.3m	£15.7m	£12.7m	£11.5m	£7.9m	£8.4m	£6.6m	£7.1m	£5.8m	**-12%**

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 12 per cent in H1 2020 compared to the same period in 2019, decreasing from £6.6 million to £5.8 million. However, the number of reported cases fell by just two per cent, highlighting that the individual loss per case has fallen notably as bank systems detect potentially fraudulent transactions at an earlier stage.

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 card company immediately.

CARD ID THEFT

OVERALL	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	CHANGE
Cases	16,329	15,427	15,772	13,384	21,350	42,441	27,963	26,202	21,108	**-25%**
Gross Loss	£20.5m	£19.5m	£15.7m	£14.1m	£17.4m	£29.9m	£18.5m	£22.8m	£15.8m	**-15%**

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 15 per cent in the first six months of 2020 compared to the same period in 2019, from £18.5 million to £15.8 million. The number of individual cases dropped by 25 per cent over the same period. While criminals are increasingly 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:

Always remember:

- 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 business of your new address.
- Destroy unwanted documents including bills, bank statements or post that's in your name, preferably by using a shedder.
- 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.

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 break down 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 as one case can cover multiple places of misuse. This can lead to double counting. 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 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	CHANGE
Gross Loss	£28.9m	£27.0m	£25.6m	£22.4m	£22.5m	£27.8m	£22.2m	£21.5m	£17.7m	**-20%**

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 with a contactless function and dropped by 20 per cent in H1 2020 compared to the first half of 2019 – the first time 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 £8.2 million of losses compared to spending of £41 billion over the same period. This is equivalent to 2.0p in every £100 spent using contactless technology, a decrease from 2.7p reported in 2019.

UK CASH MACHINE FRAUD

OVERALL	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	CHANGE
Gross Loss	£20.6m	£22.5m	£20.5m	£16.7m	£15.9m	£16.7m	£15.5m	£14.5m	£15.4m	**0%**

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

Losses at UK cash machines stayed static in the first half of 2020, compared to the same period in 2019. The majority of this fraud is thought to be perpetuated through distraction thefts and card entrapment at ATMs.

DOMESTIC AND INTERNATIONAL CARD FRAUD

OVERALL	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	CHANGE
UK Fraud	£215.2m	£202.7m	£204.9m	£202.5m	£226.7m	£269.9m	£229.3m	£269.0m	£209.0m	**-9%**
International Fraud	£106.3m	£93.9m	£81.7m	£76.2m	£79.0m	£95.8m	£84.0m	£86.7m	£79.2m	**-6%**

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 nine per cent to £209 million in H1 of this year, compared to the same period in 2019. Meanwhile international fraud losses decreased by six per cent, to £79.2 million in the first six months of this year.

The rollout of Chip & PIN technology around the world has contributed to the decreases and levels of this type of fraud remain relatively low.

UNAUTHORISED REMOTE BANKING FRAUD

OVERALL	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	CHANGE
Prevented Value	£103.2m	£102.2m	£160.2m	£100.9m	£141.9m	£175.8m	£129.8m	£139.1m	£181.5m	**40%**
Cases	17,687	15,705	18,848	15,898	15,915	15,882	18,859	25,061	29,997	**59%**
Gross Loss	£71.5m	£65.6m	£73.8m	£82.3m	£91.0m	£61.8m	£65.7m	£84.9m	£79.7m	**21%**

Remote banking fraud losses are organised into three categories: internet banking, telephone banking and mobile banking. It occurs when a criminal gains access to an individual's bank account through one of the three remote banking channels and makes an unauthorised transfer of money from the account.

Losses from remote banking fraud rose by 21 per cent in H1 2020, compared to the same period in 2019, from £65.7 million to £79.7 million. However, losses were down six per cent compared to the £84.9 million of losses in the second half of last year. The number of cases were also up 59 per cent in H1 2020 compared to H1 2019, at 29,997. Intelligence suggests fraudsters are increasingly evading banks' advanced security systems by targeting customers directly, using social engineering techniques to trick them into giving away their credentials and login details. Fraudsters will then use this information to commit fraud. A total of £181.5 million of unauthorised remote banking fraud was prevented in the first six months of the year, equivalent to £6.95 in every £10 of attempted fraud prevented.

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.
- Providing customers with free security software, which many banks offer.
- Investing in the Take Five to Stop Fraud campaign to educate customers and businesses 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 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	CHANGE
Cases	11,195	8,893	11,725	10,020	11,151	9,753	10,409	15,440	21,312	**105%**
Gross Loss	£56.1m	£45.6m	£55.5m	£65.7m	£75.6m	£47.4m	£48.8m	£63.1m	£64.3m	**32%**

This type of fraud occurs when a fraudster gains access to a customer's bank account through internet banking and makes an unauthorised transfer of money.

Losses from internet banking rose by 32 per cent in the first six months of 2020, compared to H1 2019, from £48.8 million to £64.3 million. The number of cases also increased by 105 per cent to 21,312. However, losses increased just 1.9 per cent compared to H2 2019, rising from £63.1 million to £64.3 million. A total of £144.1 million of attempted internet banking fraud was stopped by bank security systems during H1 2020. This is equivalent to £6.91 in every £10 of fraud attempted being prevented. In addition, £9.1 million (14 per cent) of the losses 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. Some banks offer free security software so check your bank's website for details.

TELEPHONE BANKING FRAUD

OVERALL	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	CHANGE
Cases	4,949	5,546	5,273	4,304	3,464	4,473	5,504	5,695	4,681	**-15%**
Gross Loss	£13.1m	£16.5m	£15.6m	£12.7m	£11.4m	£10.6m	£11.6m	£12.0m	£7.9m	**-32%**

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

Losses due to telephone banking fraud fell by 32 per cent to £7.9 million in the first six months of 2020 and the number of cases fell by 15 per cent to 4,681. A total of £32.0 million of attempted telephone banking fraud was stopped by bank security systems during H1 2020. This is equivalent to £8.02 in every £10 of fraud attempted being prevented. In addition, £0.8 million (ten per cent) of the losses 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 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	CHANGE
Cases	1,543	1,266	1,850	1,574	1,300	1,656	2,946	3,926	4,004	**36%**
Gross Loss	£2.2m	£3.5m	£2.6m	£3.9m	£4.0m	£3.8m	£5.3m	£9.9m	£7.5m	**41%**

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. 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 £7.5 million in the first six months of 2020, up 41 per cent compared to the same period in 2019. However, losses were down 25 per cent compared to the £9.9 million of losses recorded in H2 2019.

Meanwhile, the number of recorded cases rose 36 per cent. This rise reflects the growing number of customers using mobile banking – in 2019 one in two adults in the UK used mobile banking (UK Finance Payment Markets Report 2020) – and a larger offering of mobile banking facilities by banks, which has led to mobile banking becoming a renewed focus of attack for fraudsters. However, the fall in losses from H2 2019 to H1 2020 highlights the steps taken by the industry to put in place safeguards against fraudsters. A total of £5.5 million of attempted mobile banking fraud was stopped by bank security systems during H1 2020. This is equivalent to £4.23 in every £10 of fraud attempted being prevented. £0.5 million (seven per cent) of these losses across mobile banking were recovered after the incident.

How to stay safe from mobile banking fraud:

Always remember:

- Only provide organisations that you trust and have given consent to with your personal or financial details.
- Question uninvited approaches and contact companies directly using a known email or phone number.
- Contact your bank immediately if you spot transactions on your bank statements that you don't recognise.
- Just because someone knows your basic details doesn't mean they're genuine.
- Be wary of unexpected or suspicious looking pop-ups that appear during your online banking session.
- Check the online banking security options your bank may provide.

CHEQUE FRAUD

OVERALL	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H2 2019	H1 2020	CHANGE
Prevented Value	£99.8m	£96.4m	£88.8m	£123.5m	£74.3m	£143.9m	£202.3m	£348.5m	£184.2m	**-9%**
Cases	2,108	1,280	984	761	682	1338	1515	1,337	709	**-53%**
Gross Loss	£7.4m	£6.3m	£5.4m	£4.4m	£3.3m	£17.2m	£29.4m	£24.2m	£6.4m	**-78%**

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 have decreased 78 per cent in the first half of 2020, falling from £29.4 million in H1 2019 to £6.4 million in H1 2020. The number of cases also deceased, by 53 per cent.

The recent fall in cheque fraud is likely to have 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 banking industry has also worked closely with law enforcement to target the organised criminal gangs operating cheque fraud, including through a major successful **investigation** by the industry-funded Dedicated Card and Payment Crime Unit.

The value of attempted cheque fraud prevented by the banks also decreased, by nine per cent to £184.2 million in the first half of 2020, equivalent to £9.66 in every £10 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 permanent 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.

Also, in January 2018 UK Finance 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.

Since the last figures were reported two new members have also begun reporting, so the figures year on year are not directly comparable.

OVERALL AUTHORISED PUSH PAYMENT SCAMS		Personal			Non-Personal			Total		
		H1 2019	H1 2020	CHANGE	H1 2019	H1 2020	CHANGE	H1 2019	H1 2020	CHANGE
VOLUME	Total number of cases	53,475	63,186	**18%**	4,074	3,061	**-25%**	57,549	66,247	**15%**
	Total number of payments	80,440	98,145	**22%**	5,637	4,633	**-18%**	86,077	102,778	**19%**
VALUE	Total case value	£146.5m	£164.1m	**12%**	£61.0m	£43.7m	**-28%**	£207.5m	£207.8m	**0%**
	Total returned to the customer	£25.6m	£59.9m	**133%**	£13.6m	£13.2m	**-3%**	£39.3m	£73.1m	**86%**

Losses due to authorised push payment scams reached £207.8 million in the first half of 2020, static when compared to the same period in 2019. This was split between personal (£164.1 million) and non-personal or business (£43.7 million).

In total there were 66,247 cases of authorised push payment fraud in the first six months of this year. Of this total 63,186 were on personal accounts while 3,061 were on non-personal or business cases.

One case can include several payments and there was a total of 102,778 payments during the period.

While the losses recorded as a result of APP scams were flat in H1 compared to the previous year, there was a substantial increase in the funds returned to victims of APP fraud, with financial providers able to return £73.1 million in the first half of 2020, an 86 per cent increase on the sum returned in the same period in 2019.

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.

For the second time UK Finance is publishing statistics relating to the cases assessed using the voluntary code. This data covers the period 1 January 2020 until 30 June 2020.

This data shows that 61,333 cases have been assessed and closed during H1 2020 with a total value of £126.5 million, of which £47.9 million was reimbursed to victims (38 per cent of the total).

Of the 61,333 cases reported, 77 per cent involved values of less than £1,000, whilst only four per cent of cases involved the more life changing sums of £10,000 plus.

This figure does not include all money returned to APP fraud victims in all cases, for example, in some instances where the customer was found at fault under the Code but the bank was able to trace and return the original stolen funds. UK Finance and its members are working to ensure such cases are included within these figures in future fraud updates, to better reflect the total sums returned to customers in cases assessed under the Code. Currently we believe that the 'total reimbursed' figures reported under the Code are understated.

Only those cases assessed using the voluntary code by signatory PSPs
All cases reported below are already 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	47,084	11,790	2,459	61,333
	Payments	58,717	24,854	8,437	92,008
VALUE	Value	£12.1m	£37.6m	£76.7m	£126.5m
	Reimbursement	£3.6m	£13.5m	£30.8m	£47.9m

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 a 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, in May 2019 the Authorised Push Payment Voluntary Code was launched, which aims to offer greater protection for consumers who are victims of this form of fraud.

Under the terms of the 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.

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 introduction 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.
- 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 between firms and across borders to detect and prevent financial crime better.
- 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.

SCAM TYPES

PURCHASE SCAMS

PURCHASE SCAMS	H1 2019	H2 2019	H1 2020	CHANGE
Number of cases	35,472	37,864	37,516	**6%**
Number of payments	44,252	48,868	47,768	**8%**
Total value of losses	£27.9m	£31.1m	£27.1m	**-3%**
Total subsequently returned to the customer	£2.7m	£6.9m	£6.1m	**123%**

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 57 per cent of the total number of APP scam cases in the first half of 2020. The lower average case value means that they accounted for 13 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 already 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	28,341	2,783	163	31,287
	Payments	34,892	4,852	520	40,264
VALUE	Value	£6.3m	£8.1m	£3.2m	£17.7m
	Reimbursement	£1.3m	£1.6m	£1.0m	£3.8m

For only those cases which were assessed using the voluntary code, 22 per cent of all losses were returned to the victim; the smallest proportion across all eight of the scam types. 91 per cent of all cases assessed involved case values of less than £1,000.

How to stay safe from purchase scams:

- Be suspicious of any '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 are 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.

INVESTMENT SCAMS

INVESTMENT SCAMS	H1 2019	H2 2019	H1 2020	CHANGE
Number of cases	3,425	3,364	3,723	**9%**
Number of payments	7,126	7,097	9,492	**33%**
Total value of losses	£43.4m	£51.9m	£55.2m	**27%**
Total subsequently returned to the customer	£2.9m	£9.4m	£12.1m	**314%**

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. In the first six months of 2020, losses incurred as a result of investment scams rose by 27 per cent compared to H1 2019, from £43.4 million to £55.2 million. This was equivalent to 27 per cent of the total value of APP scam cases, the largest proportion of losses of all the scam categories

Only those cases assessed using the voluntary code by signatory PSPs
All cases reported below are already 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	1,338	786	671	2,795
	Payments	2,322	2,291	2,331	6,944
VALUE	Value	£0.5m	£2.9m	£28.7m	£32.2m
	Reimbursement	£0.1m	£0.6m	£9.8m	£10.6m

For only those cases which were assessed using the voluntary code, 33 per cent of all losses were refunded to the victim; in the six months before the code was introduced (Jan to June 2019) only seven per cent of losses were refunded. 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.

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 their website is genuine by checking their web address.

ROMANCE SCAMS

ROMANCE SCAMS	H1 2019	H2 2019	H1 2020	CHANGE
Number of cases	935	1,228	1,291	**38%**
Number of payments	4,388	6,629	6,170	**41%**
Total value of losses	£7.9m	£10.2m	£9.3m	**18%**
Total subsequently returned to the customer	£0.5m	£1.8m	£2.3m	**329%**

In a romance scam, the victim is convinced 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.

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 two per cent of the total number of APP scam cases in the first six months of 2020 and just over four per cent of the total value.

Only those cases assessed using the voluntary code by signatory PSPs
All cases reported below are already 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	401	332	110	843
	Payments	1,207	2,272	1,081	4,560
VALUE	Value	£0.1m	£1.3m	£3.5m	£5.0m
	Reimbursement	£0.0m	£0.4m	£1.1m	£1.5m

For only those cases which were assessed using the voluntary code, 30 per cent of all losses were refunded to the victim. In the six months before the code was introduced (Jan to June 2019) only six per cent of losses were 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 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 2019	H2 2019	H1 2020	CHANGE
Number of cases	4,601	6,110	5,680	**23%**
Number of payments	7,345	9,759	9,343	**27%**
Total value of losses	£8.2m	£9.1m	£8.0m	**-2%**
Total subsequently returned to the customer	£0.7m	£1.6m	£1.8m	**152%**

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 high-value goods – however no such payment exists. 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. Sometimes criminals ask victims to pay an upfront fee for training programmes or background checks for jobs that do not exist. Advance fee scams were the fourth most common form of APP scam in the first half of 2020, accounting for nine per cent of the total number of cases. However, by value these scams accounted for four per cent.

Only those cases assessed using the voluntary code by signatory PSPs
All cases reported below are already 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	3,794	892	81	4,767
	Payments	5,341	2,195	464	8,000
VALUE	Value	£1.2m	£2.3m	£2.8m	£6.3m
	Reimbursement	£0.3m	£0.4m	£0.8m	£1.5m

For only those cases which were assessed using the voluntary code, 24 per cent of all losses were refunded to the victim; in the six months before the code was introduced (Jan to June 2019) only eight 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 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 i.e. LinkedIn offering jobs that don't exist.
- Make sure you use a reputable recruitment company which is 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 are concerned about a job scam you can report it to a trade association and to SAFERjobs using their online reporting tool.

INVOICE AND MANDATE SCAMS

INVOICE AND MANDATE SCAMS	H1 2019	H2 2019	H1 2020	CHANGE
Number of cases	4,659	3,913	2,849	**-39%**
Number of payments	6,052	5,416	3,919	**-35%**
Total value of losses	£55.9m	£58.2m	£45.6m	**-18%**
Total subsequently returned to the customer	£13.5m	£18.8m	£18.1m	**34%**

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. Invoice and mandate scams were the second most common type of APP scam by loss seen in the first half of 2020 at £45.6 million.

This reflects the fact that the majority of losses by value were from non-personal or business accounts at £29.4 million, compared to £16.2 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 already 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	507	961	272	1,740
	Payments	594	1,174	554	2,322
VALUE	Value	£0.3m	£3.3m	£10.8m	£14.4m
	Reimbursement	£0.1m	£1.3m	£4.2m	£5.6m

For only those cases which were assessed using the voluntary code, 39 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:

Always remember:

- Confirm supplier bank details directly with suppliers using their established on-file details before any payments are made.
- Make sure you don't step outside your usual payment method even if it's urgent.
- When paying a supplier for the first time, transfer a small amount first and check payment has been received directly by the company.
- Where possible, send remittance advices to suppliers once an invoice has been paid.
- Ensure that all staff who process supplier invoices or can change bank details check for irregularities in supplier details including changes to supplier names and addresses and changes to invoiced amounts.
- Be careful with the type of information you share online about your business.
- Check your business's bank statements carefully. All suspicious debits should be reported to your bank immediately.

CEO FRAUD

CEO FRAUD	H1 2019	H2 2019	H1 2020	CHANGE
Number of cases	340	336	241	**-29%**
Number of payments	487	475	361	**-26%**
Total value of losses	£7.9m	£9.8m	£4.7m	**-40%**
Total subsequently returned to the customer	£2.1m	£1.7m	£2.2m	**1%**

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 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 2020, accounting for 241 cases – less than one 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 already 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	9	58	15	82
	Payments	10	66	27	103
VALUE	Value	£0.0m	£0.3m	£0.3m	£0.6m
	Reimbursement	£0.0m	£0.1m	£0.0m	£0.2m

For only those cases which were assessed using the voluntary code, 27 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 directly with the sender, either in person or over the phone.
- 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 STAFF	H1 2019	H2 2019	H1 2020	CHANGE
Number of cases	4,242	6,846	8,222	**94%**
Number of payments	10,056	12,204	14,478	**44%**
Total value of losses	£35.4m	£48.7m	£36.7m	**4%**
Total subsequently returned to the customer	£11.2m	£26.1m	£21.5m	**91%**

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 12 per cent of all APP scam cases in the first half of 2020. However, by value this scam was the third highest, accounting for 18 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 already 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	2,429	4,216	895	7,540
	Payments	2,998	8,328	2,406	13,732
VALUE	Value	£1.4m	£13.8m	£20.7m	£36.0m
	Reimbursement	£0.7m	£7.2m	£11.5m	£19.4m

For only those cases which were assessed using the voluntary code, 54 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:

- Remember, your bank or the police will never ask you to transfer money to a safe account, even if they say it is in your name.
- The police will never ask you to take part in an undercover operation.
- Never give anyone remote access to your computer as a result of a cold call or unsolicited message.
- If you are at all suspicious, hang up and don't reply to the message. Instead contact your bank on a number you know to be correct, such as the one the back of your bank card. You can contact your local police force via the 101 service.
- Contact your bank straight away if you think you may have fallen for an impersonation scam.
- Report to Action Fraud: If you believe you've fallen for a scam, contact your bank immediately on a number you know to be correct, such as the one listed on your statement, their website or on the back of your debit or credit card.

IMPERSONATION: OTHER

IMPERSONATION: OTHER	H1 2019	H2 2019	H1 2020	CHANGE
Number of cases	3,875	5,227	6,725	**74%**
Number of payments	6,371	8,924	11,247	**77%**
Total value of losses	£20.9m	£29.3m	£21.2m	**1%**
Total subsequently returned to the customer	£5.5m	£10.4m	£9.0m	**65%**

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. Ten per cent of all APP scam cases were due to this type of scam in the first half of 2020, also accounting for ten per cent of total losses.

Only those cases assessed using the voluntary code by signatory PSPs
All cases reported below are already 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	3,594	1,762	252	5,608
	Payments	4,682	3,676	1,054	9,412
VALUE	Value	£1.6m	£5.7m	£6.5m	£13.8m
	Reimbursement	£0.3m	£1.8m	£2.4m	£4.6m

For only those cases which were assessed using the voluntary code, 33 per cent of all losses were refunded to the victim, the third 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:

- 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, 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 victim to an impersonation scam.
- You can forward suspicious emails to **report@phishing.gov.uk** and suspected scam texts to your mobile network provider by forwarding them to 7726. If a scam text claims to be from your bank, then you should also report it to them.

PAYMENT TYPE

Payment Type	Volume				Value			
	H1 2019	H2 2019	H1 2020	CHANGE	H1 2019	H2 2019	H1 2020	CHANGE
Faster Payment	81,629	94,187	97,939	**20%**	£155.3m	£178.1m	£163.5m	**5%**
CHAPS	657	683	1,214	**85%**	£10.2m	£19.8m	£11.8m	**16%**
BACS	1,052	1,276	466	**-56%**	£13.2m	£18.3m	£13.8m	**5%**
Intra Bank transfer	612	1,353	650	**6%**	£1.0m	£2.6m	£0.8m	**-26%**
International	2,127	1,873	2,509	**18%**	£27.9m	£29.5m	£18.1m	**-35%**
Total	**86,077**	**99,372**	**102,778**	**19%**	**£207.5m**	**£248.3m**	**£207.8m**	**0%**

This data shows the type of payment method the victim used to make the authorised push payment. Faster Payment was used in 95 per cent of cases and accounted for 79 per cent of losses by value.

PAYMENT CHANNEL

Payment Channel	Volume				Value			
	H1 2019	H2 2019	H1 2020	CHANGE	H1 2019	H2 2019	H1 2020	CHANGE
Branch	6,533	4,539	3,335	**-49%**	£24.2m	£24.9m	£20.3m	**-16%**
Internet Banking	58,147	61,077	53,566	**-8%**	£158.6m	£186.1m	£146.3m	**-8%**
Telephone Banking	2,248	3,753	2,775	**23%**	£12.0m	£15.5m	£13.1m	**9%**
Mobile Banking	19,149	30,003	43,102	**125%**	£12.7m	£21.8m	£28.1m	**122%**
Total	**86,077**	**99,372**	**102,778**	**19%**	**£148.2m**	**£206.1m**	**£207.8m**	**0%**

This data shows the channel through which the victim made the authorised push payment. Internet banking was used in 52 per cent of cases and accounted for 70 per cent of losses incurred.

UK Finance is urging customers to follow the advice of the Take Five to Stop Fraud campaign, and remember that criminals are experts at impersonating people, organisations and the police.

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