UK FINANCE

2019 HALF YEAR FRAUD UPDATE

ukfinance.org.uk

INTRODUCTION

Fraud continues to be a hugely topical issue, with the banking and finance industry investing ever more time and money in fighting economic crime and educating consumers to help protect them against fraudsters.

We work with government, law enforcement, regulators and increasingly other sectors such as telecommunications, to detect and prevent fraud at the earliest stage possible.

Yet criminals are constantly adapting the methods they use to gain illicit funds and con innocent victims into falling prey to scams.

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

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

In an authorised fraud push payment fraudulent transaction, the genuine customer themselves processes a payment to another account which is controlled by a criminal.

In the first half of 2019, losses due to unauthorised financial fraud on payment cards, remote banking and cheques rose two per cent, to £408.3 million.

In the first half of 2019, a total of £207.5 million was lost to authorised push payment scams. While the figures year on year are not directly comparable as more banks are now reporting on APP, the increasing focus of criminals on these scams has helped to drive a 40 per cent increase in losses compared to the same period in 2018.

The banking and finance industry is committed to tackling fraud and scams by:

- Investing in advanced security systems to protect customers, including real-time transaction analysis, behavioral biometrics on devices and technology to identify the different sound tones that every phone has and the environment that they are in.
- 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 operational in every police force area and prevented £23.2 million of fraud and enabled 134 arrests in the first half of 2019.

- Sponsoring a specialist police unit, the Dedicated Card and Payment Crime Unit (DCPCU), which tackles the organised criminal groups responsible for financial fraud and scams. In the first half of 2019, the unit prevented an estimated £6.8 million of fraud, secured 39 convictions and disrupted 13 organised crime groups (OCGs).

- The introduction of 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 the Mule Insights Tactical Solution (MITS), a technology that helps to track suspicious payments and identify money mule accounts.

- Working with Pay.UK to implement Confirmation of Payee (CoP), an account name checking service for when a payment is being made that will help to prevent authorised push payment scams.

- Working with the Financial Conduct Authority (FCA) on the phased implementation of Strong Customer Authentication (SCA), new EU-wide rules aimed at reducing fraud by verifying a customer's identify when they make certain higher value online purchases. These rules began to be rolled out in September 2019.

- Hosting and part-funding the government-led programme to reform the system of economic crime information sharing, known in the industry as Suspicious Activity Reports (SARs), so that it meets the needs of crime agencies, regulators, consumers and businesses.

- Helping customers stay safe from fraud and spot the signs of a scam through the Take Five to Stop Fraud campaign, in collaboration with the Home Office.

The advice of the Take Five to Stop Fraud campaign warns customers to:

- **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.

OUR FRAUD DATA

We collect fraud data relating to two different areas - authorised fraud and unauthorised fraud.

Authorised fraud
In an authorised fraud push payment fraudulent transaction, the genuine customer themselves processes a payment to another account which is controlled by a criminal.

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

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.

For only the third time (the first was in 2018), UK Finance is reporting enhanced data on APP scams.

Some caveats are required for the tables in the document:

- 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 revised data being presented by members.
- Figures in the tables are rounded to the nearest £0.1m. The percentage change figures from H1 2018 and H1 2019 included in the tables are calculated using actual losses.

UNAUTHORISED FRAUDULENT TRANSACTIONS:

JANUARY TO JUNE 2019 (CARDS, CHEQUES & REMOTE BANKING)

OVERALL	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H1 18/H1 19%
Prevented value	£939.5m	£821.5m	£678.7m	£708.9m	£751.4m	£706.8m	£717.6m	£944.7m	£820.2m	**14%**
Cases	610,225	816,019	937,274	920,232	936,699	973,308	1,198,130	1,453,426	1,385,447	**16%**
Gross Loss	£320.3m	£435.3m	£400.4m	£368.4m	£365.8m	£365.5m	£400.0m	£444.8m	£408.3m	**2%**

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 reached £408.3 million in the first half of this year, an increase of two per cent on the previous year. The number of recorded cases of unauthorised fraudulent transactions rose by 16 per cent to 1.39 million.

However, losses were £36 million lower than those recorded in the second half of 2018, as banks continue to invest in fighting fraud.

There was a 14 per cent increase in prevented fraud in H1 2019, with banks stopping £820.2 million of attempted unauthorised fraudulent transactions. This equates to the industry preventing £6.68 in every £10 of attempted fraud, or £4.5 million a day.

AUTHORISED PUSH PAYMENT (APP) SCAMS:

JANUARY TO JUNE 2019

OVERALL	H1 2018	H2 2018	H1 2019	H1 18/H1 19%
Total number of cases	34,129	50,495	57,549	69%
Total case value	£148.2m	£206.1m	£207.5m	40%
Total returned to the customer	£30.9m	£51.7m	£39.3m	27%

Total losses due to authorised push payment scams were £207.5 million in the first half of 2019. There were 57,549 cases. This data is not directly comparable with the figures for the same period last year.

There was an increase in the number of cases reported in every scam category, with purchase scams rising 65 per cent to 35,472. Cases of impersonation scams more than doubled, while the number of investment scam cases rose 152 per cent.

There was a slight fall in the amount returned to victims, from 21 per cent in the first half of 2018, to 19 per cent in the first six months of 2019. 60 per cent of cases are resolved in under a week. These figures are separate from the voluntary code on APP scams which only came into force on 28 May 2019. Separate data on decision times under the APP code is due to be published in UK Finance's annual fraud report which is scheduled to come out in 2020.

WHAT IS DRIVING FRAUD LOSSES?

Criminals are constantly adapting their methods 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 money. While it is not possible to be specific about the value of fraud that can be attributed to individual methods of compromise, intelligence reported by our members points to the main drivers.

Fraud losses are being driven by the theft of customers' personal and financial data through a range of methods. Customer details are often stolen through data breaches at third parties outside the financial sector. Fraudsters also continue to use social engineering techniques to trick customers into divulging their personal information or transferring money.

> *"Data breaches continue to be a key enabler of fraud. Personal and financial information obtained in a breach can be used to commit frauds affecting individuals, the private and public sectors alike. By harvesting personal and financial information through data breaches, criminals are able to commit fraud and damage people, businesses and services."*
>
> National Crime Agency website, 2019

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 authority.

One area of fraud that has seen a significant rise is investment scams. These are having an increasing impact on the number of cases seen and the associated total losses, with our 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 cloned sites during online searches for investment opportunities. Scammers are also increasingly using social media sites to entice victims by advertising fake investments.

Criminals also steal data by intercepting mail or using malware and phishing. 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 stole data.

Increasingly 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 who use it to commit remote purchase fraud. These attacks continue to highlight the importance of online retailers implementing and maintaining robust security measures.

Meanwhile intelligence also suggests criminals continue to use more low-tech methods such as distraction thefts and card entrapments to steal debit and credit cards which are then used to commit fraud.

UNAUTHORISED DEBIT AND CREDIT AND OTHER PAYMENT CARD FRAUD

OVERALL	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H1 18/H1 19%
Prevented value	£366.3m	£477.3m	£475.7m	£510.3m	£502.4m	£482.4m	£501.4m	£625.0m	£488.2m	**-3%**
Cases	593,417	793,775	917,479	903,247	916,867	956,649	1,181,533	1,436,206	1,365,112	**16%**
Gross Loss	£244.6m	£323.5m	£321.5m	£296.5m	£286.7m	£278.8m	£305.7m	£365.7m	£313.3m	**2%**

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 £313.3 million in the first half of 2019, an increase of two per cent on the same period in 2018.

Over this period, the overall value of card spending grew by 2.6 per cent to £86.5 billion. Card fraud as a proportion of card purchases has increased from 7.6p in the first half of 2018 to 8.4p in the first half of 2019.

A total of £488.2 million of card fraud was stopped by banks and card companies in the first six months of 2019, a decrease of three per cent on the same period in 2018. This is equivalent to £6.09 in every £10 of attempted card fraud being prevented without a loss occurring.

Meanwhile, losses from counterfeit card fraud were down 16 per cent compared to the same period a year ago, with the lowest total ever reported. The significant decrease in this type of fraud is likely to be the result of the previous introduction of chip technology in the UK and its subsequent increased adoption around the world, most notably in the United States.

Fraud using the contactless functionality on cards and devices remains low, with £10.2 million of losses during H1 2019, compared to spending of £38 billion over the same period. This is equivalent to 2.7p in every £100 spent using contactless technology, the same level recorded in 2018 and 2017. Fraud using the contactless technology on payment cards and devices represents just three per cent of overall card fraud losses.

There has never been a verified report in the UK of a fraudster taking money from someone's contactless card just by bumping into them in the street or on public transport. The only information detectable from scanning a card is the card number and expiry date, the security code on the back cannot be accessed via these devices. As the vast majority of online retailers require additional details like these to make a purchase, there is very little chance of fraudsters being able to make online transactions.

The finance industry is tackling card fraud by:

- Investing in advanced security systems to protect customers, including real-time transaction analysis, behavioral biometrics on devices and technology to identify the different sound tones that every phone has and the environment that they are in.

- The introduction of Strong Customer Authentication (SCA) which began with a phased rollout in September of this year. It will see new requirements introduced for online payments, as well as contactless transactions, in order to make them even more secure and protect against fraudsters.

- Sponsoring the specialist police unit, the Dedicated Card and Payment Crime Unit (DCPCU) which tackles the criminal gangs behind fraud.

REMOTE PURCHASE FRAUD

OVERALL	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H1 18/H1 19 %
Cases	473,504	639,580	728,087	709,745	703,729	694,424	922,515	1,127,760	1,071,493	**16%**
Gross Loss	£171.7m	£226.7m	£224.1m	£208.2m	£204.8m	£203.6m	£231.8m	£274.6m	£237.4m	**2%**

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 rose two per cent to £237.4 million in the first six months of 2019. However, at the same time the number of cases rose by 16 per cent, resulting in a lower average case value. This indicates 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 £181.9 million in the first half of 2019, an increase of two per cent when compared to the same period in 2018.

Staying safe from remote purchase fraud:

- If you're using a retailer for the first time, always take time to research them before you give them any of your details. Be prepared to ask questions before making a payment.
- If an offer looks too good to believe then it probably is. Be suspicious of prices that are too good to be true.
- Only use retailers you trust, for example ones you know or have been recommended to you. If you're buying an item made by a major brand, you can often find a list of authorised sellers on their official website.
- Take the time to install the built-in security measures most browsers and many banks offer.

LOST AND STOLEN CARD FRAUD

OVERALL	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H1 18/ H1 19 %
Cases	61,500	82,302	109,110	122,054	148,474	201,805	204,862	230,129	230,727	**13%**
Gross Loss	£30.3m	£43.8m	£49.5m	£46.8m	£47.8m	£45.1m	£45.5m	£49.6m	£48.3m	**6%**

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 type of fraud rose six per cent in H1 of this year to £48.3 million. This was three per cent down from £49.6 million in the second half of 2018. Meanwhile the number of incidents rose 13 per cent in H1 2019 compared to H1 2018, resulting in a lower average loss per individual case. This reflects that bank systems are detecting fraudulent spending more quickly, combined with the £30 limit on individual contactless transactions. Each contactless card also has an inbuilt security feature, which means from time to time cardholders making a contactless transaction will be asked to enter their PIN to prove they are in possession of their card.

New rules being rolled out will require customers to enter this PIN once they have made payments exceeding roughly £130, or after five contactless payments have been made.

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. However, a new modus operandi is also being used, with distraction thefts also 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 2015	H2 2015	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H1 18/ H1 19 %
Cases	5,033	5,686	5,685	5,692	5,466	5,437	4,697	5,349	3,949	**-16%**
Gross Loss	£5.7m	£5.9m	£6.1m	£6.4m	£5.6m	£4.6m	£3.0m	£3.3m	£2.5m	**-18%**

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 18 per cent in the first six months of 2019 to £2.5 million, with the number of individual cases also dropping by 16 per cent. 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 this 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 2015	H2 2015	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H1 18/ H1 19 %
Cases	39,711	46,310	58,268	50,329	43,426	41,599	28,109	30,527	30,980	**10%**
Gross Loss	£19.8m	£25.9m	£21.3m	£15.7m	£12.7m	£11.5m	£7.9m	£8.4m	£6.6m	**-16%**

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 16 per cent in H1 2019 compared to the same period in 2018, decreasing from £7.9 million to £6.6 million; the lowest half-year total ever reported. However, the number of reported cases rose by ten per cent, which means 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, wallet 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 2015	H2 2015	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H1 18/ H1 19 %
Cases	13,669	19,897	16,329	15,427	15,772	13,384	21,350	42,441	27,963	**31%**
Gross Loss	£17.1m	£21.1m	£20.5m	£19.5m	£15.7m	£14.1m	£17.4m	£29.9m	£18.5m	**6%**

This type of fraud occurs in two ways, through third-party applications or account takeover.

Third-party application fraud occurs when criminals 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.

Account takeover fraud occurs when 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 rose six per cent in the first six months of 2019 compared to the same period in 2018, from £17.4 million to £18.5 million. However, the number of individual cases rose by 31 per cent over the same period. This indicates that criminals are increasingly using this form of fraud to open accounts in other people's names but 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 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 2015	H2 2015	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H1 18/ H1 19 %
Gross Loss	£23.0m	£30.6m	£31.8m	£31.0m	£31.2m	£30.7m	£31.4m	£38.4m	£32.4m	**3%**

UK retail face-to-face fraud covers all transactions that occur in person in a UK shop. Fraud losses on face-to-face purchases on the UK high street increased three per cent in H1 2019 to £32.4 million.

The majority of this fraud is undertaken by fraudsters using low-tech techniques to steal the card, and often the PIN, to carry out fraudulent transactions in shops. This includes criminals using methods such as ATM card entrapment and distraction thefts, combined with shoulder surfing and PIN pad cameras. Criminals also use methods to dupe victims into handing over their cards on their own doorstep.

This category also includes fraud incidents involving the contactless functionality on both payment cards and devices. Fraud using the contactless functionality on cards and devices remains low, with £10.2 million of losses during H1 2019, compared to spending of £38 billion over the same period. This is equivalent to 2.7p in every £100 spent using contactless technology, the same level recorded in 2018 and 2017. Fraud using the contactless technology on payment cards and devices represents just three per cent of overall card fraud losses.

UK CASH MACHINE FRAUD

OVERALL	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H1 18/ H1 19 %
Gross Loss	£14.9m	£17.8m	£20.6m	£22.5m	£20.5m	£16.7m	£15.9m	£16.7m	£15.5m	**-3%**

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

Losses at UK cash machines fell three per cent to £15.5 million in the first half of 2019, compared to the same period in 2018.

While most of this fraud is thought to be perpetuated through distraction thefts and card entrapment at ATMs, the decrease in losses suggests that consumers are becoming more aware of the need to take precautions.

DOMESTIC AND INTERNATIONAL CARD FRAUD

OVERALL	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H1 18/ H1 19 %
UK Fraud	£164.6m	£215.1m	£215.2m	£202.7m	£204.9m	£202.5m	£226.7m	£269.9m	£229.3m	**1%**
International Fraud	£80.1m	£108.4m	£106.3m	£93.9m	£81.7m	£76.2m	£79.0m	£95.8m	£84.0m	**6%**

These figures provide a breakdown of fraud committed on a UK-issued payment card, split between whether the incident occurred in the UK or internationally.

UK card fraud losses rose marginally – by one per cent to £229.3 million – in H1 of this year, compared to the same period in 2018. Meanwhile international fraud losses increased by six per cent, to £84.0 million in the same period.

The roll out of Chip & PIN technology around the world has helped to keep levels relatively low, with a reduction of 27 per cent when compared to the peak of £115.1 million reported in 2008. This fall relates to international card losses.

UNAUTHORISED BANKING FRAUD

OVERALL	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H1 18/ H1 19 %
Prevented Value	£311.3m	£213.3m	£103.2m	£102.2m	£160.2m	£100.9m	£141.9m	£175.8m	£129.7m	**-9%**
Cases	13,971	19,335	17,687	15,705	18,848	15,898	15,915	15,882	18,820	**18%**
Gross Loss	£66.2m	£102.4m	£71.5m	£65.6m	£73.8m	£82.3m	£91.0m	£61.8m	£65.7m	**-28%**

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 fell by 28 per cent in H1 2019, compared to the same period in 2018, from £91.0 million to £65.7 million. However, the number of cases was up 18 per cent over the same period to 18,820. The increase in cases combined with a decrease in losses is a good indication that banks are getting better at stopping this type of fraud. Evidence also suggests that there has been a migration away by fraudsters who are now preferring to target the victims into transferring money themselves.
A total of £129.7 million of unauthorised remote banking fraud was prevented in the first six months of the year, equivalent to £6.63 in every £10 of attempted fraud prevented.

In addition, 20 per cent (£13.1 million) of the losses across all remote banking channels were recovered after the incident.

The finance industry is tackling remote banking fraud by:

- Continuously investing in advanced security systems, including sophisticated ways of authenticating customers, such as 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 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 2015	H2 2015	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H1 18/ H1 19 %
Cases	8,417	11,274	11,195	8,893	11,725	10,020	11,151	9,753	10,352	**-7%**
Gross Loss	£50.4m	£83.1m	£56.1m	£45.6m	£55.5m	£65.7m	£75.6m	£47.4m	£48.7m	**-36%**

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 from it. Losses from internet banking fell by 36 per cent in the first six months of 2019, compared to H1 2018, from £75.6 million to £48.7 million. The number of cases also decreased by seven per cent to 10,352.

This type of fraud is facilitated by criminals' use of social engineering tactics to trick customers into revealing their internet banking security details. These include impersonation scams using phone calls, texts and emails which often claim there has been suspicious activity on a bank account, that account details need to be updated or verified or that a refund is due. The stolen details are then used to access a customer's online account and to make an unauthorised transaction.

Intelligence suggests that preventative tools put in place to prevent consumers becoming a victim of internet banking fraud have resulted in fraudsters preferring to target victims into making payments themselves, this in part is evidenced by the rises in authorised push payment fraud.

In addition, 24 per cent (£11.5 million) of the losses in the internet banking channel 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 2015	H2 2015	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H1 18/ H1 19 %
Cases	4,777	6,603	4,949	5,546	5,273	4,304	3,464	4,473	5,522	**59%**
Gross Loss	£14.7m	£17.6m	£13.1m	£16.5m	£15.6m	£12.7m	£11.4m	£10.6m	£11.6m	**2%**

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.

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

Losses due to telephone banking fraud rose by two per cent to £11.6 million in the first six months of 2019. However, the number of cases rose by 59 per cent to 5,522. These figures demonstrate that despite an increase in attempts by criminals to carry out telephone banking fraud, such frauds are being detected at an earlier stage — this is due to technologies such as voice biometrics or those which recognise the different sound tones that every phone has and the environment they are in — preventing greater sums of money from being stolen.

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

How to stay safe from telephone banking fraud:

- Never disclose security details, such as your full banking password. A genuine financial provider or organisation will never ask you for these in an email, on the phone 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 2015	H2 2015	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H1 18/ H1 19 %
Cases	777	1,458	1,543	1,266	1,850	1,574	1,300	1,656	2,946	**127%**
Gross Loss	£1.0m	£1.8m	£2.2m	£3.5m	£2.6m	£3.9m	£4.0m	£3.8m	£5.3m	**33%**

Mobile banking fraud occurs when a criminal uses compromised bank account details to gain access to a customer's bank account through a banking app downloaded to a mobile device only. It excludes 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 £5.3 million in the first six months of 2019, up 33 per cent compared to the same period in 2018. Meanwhile, the number of recorded cases rose 127 per cent. This rise reflects the growing number of customers using mobile banking and a larger offering of mobile banking facilities by banks.

UK Finance's latest UK Payment Markets report found that almost half (48 per cent) of UK adults used mobile banking in 2018, up from 41 per cent the previous year, while bank payments made using internet or mobile banking in 2018 grew to two billion, up from 1.6 billion in 2017.

Nine per cent (£0.5 million) of the losses in the mobile banking channel 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 2015	H2 2015	H1 2016	H2 2016	H1 2017	H2 2017	H1 2018	H2 2018	H1 2019	H1 18/ H1 19 %
Prevented Value	£262.0m	£130.9m	£99.8m	£96.4m	£88.8m	£123.5m	£74.3m	£143.9m	£202.3m	**172%**
Cases	2,837	2,909	2,108	1,280	984	761	682	1,338	1,515	**122%**
Gross Loss	£9.5m	£9.4m	£7.4m	£6.3m	£5.4m	£4.4m	£3.3m	£17.2m	£29.4m	**789%**

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

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

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

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

Losses from cheque fraud increased by 789 per cent in the first half of 2019, rising from £3.3 million in H1 2018 to £29.4 million in H1 2019. The number of cases also grew, by 122 per cent. Intelligence suggests the increase was almost entirely down to criminals targeting business accounts, where losses per case are higher, with personal customers only accounting for a small fraction of the total losses. Specifically, there has been a relatively small increase in counterfeit fraud on high-value business cheques.

The value of attempted cheque fraud prevented by the banks also rose substantially, by 172 per cent to £202.3 million in the first half of 2019, up from £74.3 million over the same period in 2018. This is equivalent to £8.73 in every £10 if fraud attempted being stopped without a loss occurring.

How to stay safe from cheque fraud:

- Always complete cheques using a ballpoint pen, or pen with indelible ink.
- Draw a line through all unused spaces, including after the payee name.
- Keep your chequebook in a safe place, report any missing cheques to your bank immediately and always check your bank statement thoroughly.
- Businesses should adopt anti-fraud features, such as printing cheques on security watermark paper.
- Store company cheques in business secure locations.

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 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 also led to a notable increase in the reported cases of APP fraud.

Since the last figures were published additional members have also begun reporting, so the figures year on year are not directly comparable.

Overall Authorised push payments scams		Personal			
		H1 2018	H2 2018	H1 2019	H1 18 / H1 19 %
Volume	Total number of cases	31,510	46,705	53,475	70%
	Total number of payments	47,346	67,361	80,440	70%
Value	Total case value	£92.9m	£135.4m	£146.5m	58%
	Total returned to the customer	£15.4m	£26.9m	£25.6m	66%

Overall Authorised push payments scams		Non-Personal			
		H1 2018	H2 2018	H1 2019	H1 18 / H1 19 %
Volume	Total number of cases	2,619	3,790	4,074	56%
	Total number of payments	3,618	5,332	5,637	56%
Value	Total case value	£55.3m	£70.7m	£61.0m	10%
	Total returned to the customer	£15.5m	£24.8m	£13.6m	-12%

Overall Authorised push payments scams		Total			
		H1 2018	H2 2018	H1 2019	H1 18 / H1 19 %
Volume	Total number of cases	34,129	50,495	57,549	69%
	Total number of payments	50,964	72,693	86,077	69%
Value	Total case value	£148.2m	£206.1m	£207.5m	40%
	Total returned to the customer	£30.9m	£51.7m	£39.3m	27%

Losses due to APP scams reached £207.5 million in the first half of 2019, split between personal (£146.5 million) and non-personal or business (£61.0 million). This is an increase of 40 per cent compared to the same period in 2018, although the figures are not directly comparable, as said previously, because two additional members began reporting the data to UK Finance from early 2019. In addition, intelligence suggests that increased public awareness in the build-up to the introduction of the Authorised Push Payment Scams Voluntary Code has resulted in an increase in reporting by customers who fall victim to this type of fraud.

In total there were 57,549 cases of APP fraud in the first six months of this year. Of this total 53,475 were on personal accounts while 4,074 were on non-personal or business accounts.

One case can include several payments and there was a total of 86,077 fraudulent authorised push payments during the period.

> *“Financial firms quite reasonably question why they have to pick up the bill for fraud in the system, when so much of it would not be possible without data breaches and other actions by firms outside the financial sector.”*
>
> Charles Randell, Financial Conduct Authority, September 2019

Of the losses seen as a result of APP fraud financial providers were able to return £39.3 million in the first half of 2019, a 27 per cent increase on the sum returned in the same period in 2018. However, the figures for the first half of this year reflect just one month of the APP Voluntary Code.

In an APP 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, at the end of May the Authorised Push Payment Voluntary Code was launched, which aims to offer greater protection for consumers who are victims of this form of fraud.

Firms who have signed up to the code have committed to reimbursing the victims of these scams, provided the customer has met the standards expected of them under the code. In situations where both the customer and their payment service provider meet the requirements set out in the code, a customer of a signatory firm who falls victim to an APP scam will still receive their money back.

To date eight major providers covering 17 consumer brands, and over 85 per cent of authorised push payments, have signed up, including Barclays, HSBC, Lloyds, RBS and Santander.

The finance industry is tackling APP scams by:

- Introducing new standards for payment service providers (PSPs) under the APP voluntary code, including providing effective warnings to customers if the bank identifies an APP fraud risk.
- Helping to prevent customers being duped by criminals by raising awareness of how to stay safe through the Take Five to Stop Fraud campaign, in conjunction with the Home Office.
- The implementation of an industry code for the reimbursement of victims of authorised push payment scams.
- Implementing best practice 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 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 2019 prevented £23.2 million of fraud and led to 134 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.
- Hosting the government-led programme to reform the system of economic crime information sharing, known in the industry as Suspicious Activity Reports, so that it meets the needs of crime agencies, regulators, consumers and businesses.
- Working with Pay.UK to implement the Mule Insights Tactical Solution (MITS), a technology that helps to track suspicious payments and identify money mule 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).
- Five payment types: Faster Payment, CHAPS, BACS, 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.

There are more detailed figures available in the tables in the annexe to this document.

SCAM TYPES

PURCHASE SCAMS

Purchase scams	H1 2018	H2 2018	H1 2019	H1 18 / H1 19 %
Number of cases	21,483	31,138	35,472	65%
Number of payments	27,011	39,685	44,252	64%
Total value of losses	£19.4m	£26.9m	£27.9m	43%
Total subsequently returned to the customer	£1.6m	£2.6m	£2.7m	73%

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. They will then typically persuade their victim to pay via a bank transfer, rather than the secure payment options most online platforms offer.

Purchase scams were a very common form of APP scam, accounting for more than 60 per cent (61.6) of the total number of APP scam cases in the first half of 2019. The lower average case value means that they accounted for 13 per cent of the total value of APP scams in the same period.

How to stay safe from purchase scams:

- Trust your instincts. Be suspicious of any offers or prices that look too good to be true.
- Always use the secure payment method recommended by reputable online retailers and auction websites. Be very wary of requests to pay by bank transfer.
- Do your research and ask questions before you buy. Ask to see any vehicle in person first and request the relevant documentation to ensure the seller owns it.
- If you're buying an item made by a major brand, you can often find a list of authorised sellers on their official website.
- Contact your bank straight away if you think you may have fallen victim to a purchase scam.

INVESTMENT SCAMS

Investment scams	H1 2018	H2 2018	H1 2019	H1 18 / H1 19 %
Number of cases	1,359	2,026	3,425	152%
Number of payments	3,675	4,261	7,126	94%
Total value of losses	£20.8m	£29.3m	£43.4m	108%
Total subsequently returned to the customer	£1.4m	£2.5m	£2.9m	114%

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 2019 losses incurred as a result of investment scams rose by 108 per cent compared to H1 2018, from £20.8 million to £43.4 million. This was equivalent to 20 per cent of the total value of APP scam cases.

Investment scams accounted for the largest proportion of losses among personal customers, with £41 million lost to this type of fraud, or over £12,200 per case.

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. Scammers are also known to send out paperwork with the legitimate address to send back to, to add a layer of credibility. In many cases the victim does not realise it is a scam until the first return on investment is not received.

The banking and finance industry is working closely with law enforcement to ensure cloned websites used by fraudsters are taken down.

How to stay safe from investment scams:

- Be wary of any unsolicited approaches offering investment opportunities – genuine investment companies do not cold call people.
- Check with the Financial Conduct Authority to see if a firm is authorised or registered with them before making any investment. This can be done through the FCA's ScamSmart campaign which allows consumers to check potential investment and pensions scams against a FCA Warning List.
- Watch out for any too good to be true investment opportunities. If you are being pressurised to invest quickly it a sign that it could be a scam.
- Contact your bank straight away if you think you may have fallen victim to an investment scam.

ROMANCE SCAMS

Romance scams	H1 2018	H2 2018	H1 2019	H1 18 / H1 19 %
Number of cases	571	833	935	64%
Number of payments	3,372	4,202	4,388	30%
Total value of losses	£5.3m	£7.3m	£7.9m	50%
Total subsequently returned to the customer	£0.3m	£0.3m	£0.5m	68%

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 less than two per cent of the total number of APP scam cases in the first six months of 2019 and just under four per cent of the total value.

How to stay safe from romance scams:

- Be suspicious of any requests for money from someone you have never met in person, particularly if you have only recently met. Speak to your family or friends to get advice.
- Profile photos may not be genuine, do your research first.
- Contact your bank straight away if you think you may have fallen victim to a romance scam.

ADVANCE FEE SCAMS

Advance fee scams	H1 2018	H2 2018	H1 2019	H1 18 / H1 19 %
Number of cases	3,646	4,487	4,601	26%
Number of payments	6,045	7,226	7,345	22%
Total value of losses	£5.9m	£8.0m	£8.2m	38%
Total subsequently returned to the customer	£0.5m	£0.9m	£0.7m	49%

In an advance fee scam, a criminal convinces their victim to pay a fee which would they claim would 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.

Advance fee scams were the third most common form of APP scam in the first half of 2019, accounting for eight per cent of the total number of cases. However, by value these scams accounted for just four per cent.

How to stay safe from advance fee scams:

- Be suspicious of any claims that you are due money or goods which you have not ordered or were aware of, especially if you are being asked to make a payment.
- If you have not entered a lottery or competition, then it is extremely unlikely you have won anything.
- Contact your bank straight away if you think you may have fallen victim to an advance fee scam.

INVOICE AND MANDATE SCAM

Invoice and Mandate scams	H1 2018	H2 2018	H1 2019	H1 18 / H1 19 %
Number of cases	2,857	4,697	4,659	63%
Number of payments	3,703	6,195	6,052	63%
Total value of losses	£52.1m	£71.7m	£55.9m	7%
Total subsequently returned to the customer	£13.2m	£23.2m	£13.5m	2%

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 seen in the first half of 2019 and accounted for the largest share of losses, at £55.9 million.

This reflects the fact that most losses by value were from non-personal or business accounts at £41.7 million, compared to £14.2 million of losses seen against personal accounts. Typically, corporate invoices will be larger than personal invoices and therefore a more attractive target for fraudsters.

How to stay safe from invoice and mandate scams:

- Always confirm any bank account details directly with the company either on the telephone or in person before you make a payment.
- Criminals can access or alter emails to make them look genuine. Do not use the contact details in an email, instead check the company's official website or documentation.
- If you are making a payment to an account for the first time, transfer a small sum first and then check with the company that the payment has been received to check the account details are correct.
- Contact your bank straight away if you think you may have fallen victim to an invoice or mandate scam.

CEO FRAUD

CEO fraud	H1 2018	H2 2018	H1 2019	H1 18 / H1 19 %
Number of cases	347	256	340	-2%
Number of payments	478	353	487	2%
Total value of losses	£8.0m	£6.8m	£7.9m	-1%
Total subsequently returned to the customer	£2.2m	£2.1m	£2.1m	-2%

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 another senior executive 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 2019, accounting for 340 cases – less than one per cent of the total and accounted for four per cent of total losses.

How to stay safe from CEO fraud:

- Always check any unusual payment requests directly, ideally in person or by telephone, to confirm the instruction is genuine. Do not use contact details from the email.
- Establish a documented internal process for requesting and authorising all payments and be suspicious of any request to make a payment outside of the company's standard process.
- Be cautious about any unexpected emails which request urgent bank transfers, even if the message appears to have originated from someone from your own organisation.
- Contact your bank straight away if you think you may have fallen victim to CEO fraud.

IMPERSONATION: POLICE/BANK STAFF

Impersonation: Police/Bank staff	H1 2018	H2 2018	H1 2019	H1 18 / H1 19 %
Number of cases	1,947	3,512	4,242	118%
Number of payments	3,196	5,507	10,056	215%
Total value of losses	£22.2m	£34.3m	£35.4m	60%
Total subsequently returned to the customer	£6.9m	£12.9m	£11.2m	63%

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 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 seven per cent of all APP scam cases in the first half of 2019. However, by value this scam was the third highest, accounting for 17 per cent of total losses. This highlights the need for the police to also promote the fraud awareness messaging.

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 on 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 victim to an impersonation scam.

IMPERSONATION: OTHER

Impersonation: Other	H1 2018	H2 2018	H1 2019	H1 18 / H1 19 %
Number of cases	1,919	3,546	3,875	102%
Number of payments	3,484	5,264	6,371	83%
Total value of losses	£14.4m	£21.8m	£20.9m	45%
Total subsequently returned to the customer	£4.9m	£7.0m	£5.5m	13%

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 to settle a fictitious fine or to return an erroneous refund. The scams can often involve the criminal requesting remote access to the victim's computer.

Seven per cent of all APP scam cases were due to this type of scam in the first half of 2019, accounting for ten per cent of total losses.

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.

PAYMENT TYPE

Payment Type	Volume				Value			
	H1 2018	H2 2018	H1 2019	H1 18 / H1 19 %	H1 2018	H2 2018	H1 2019	H1 18 / H1 19 %
Faster Payment	47,515	67,817	81,629	72%	£99.4m	£152.3m	£155.3m	56%
CHAPS	357	295	657	84%	£13.3m	£12.7m	£10.2m	-23%
BACS	597	857	1,052	76%	£9.5m	£14.1m	£13.2m	38%
Intra Bank transfer	921	801	612	-34%	£2.0m	£1.3m	£1.0m	-50%
International	1,574	2,923	2,127	35%	£24.0m	£25.9m	£27.9m	16%
Total	50,964	72,693	86,077	69%	£148.2m	£206.1m	£207.5m	40%

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 75 per cent of losses by value.

PAYMENT CHANNEL

Payment Channel	Volume				Value			
	H1 2018	H2 2018	H1 2019	H1 18 / H1 19 %	H1 2018	H2 2018	H1 2019	H1 18 / H1 19 %
Branch	3,344	4,575	6,533	95%	£18.9m	£22.3m	£24.2m	28%
Internet Banking	39,155	54,311	58,147	49%	£120.0m	£168.6m	£158.6m	32%
Telephone Banking	2,278	2,243	2,248	-1%	£6.1m	£8.7m	£12.0m	97%
Mobile Banking	6,187	11,564	19,149	210%	£3.1m	£6.4m	£12.7m	305%
Total	50,964	72,693	86,077	69%	£148.2m	£206.1m	£207.5m	40%

This data shows the channel through which the victim made the authorised push payment. Internet banking was used in 68 per cent of cases and accounted for 76 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. 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