# 2018 half year fraud update:

## Unauthorised payment card, remote banking and cheque fraud and authorised push payment scams

September 2018

The threat from fraud is always changing, but the finance industry is continuously enhancing its response, with investment in detection and verification systems to protect customers and collaboration with government and law enforcement to stop the criminals.

UK Finance publishes data on losses due to unauthorised fraudulent transactions made using payment cards, online and telephone 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 is duped into making the payment to be made to another account.

In the first half of 2018, losses due to unauthorised financial fraud on payment cards, remote banking and cheques fell by 2 per cent to £358.0 million.

In the first half of 2018, a total of £145.4 million was lost due to authorised push payment scams. This is 44 per cent higher than in the same period of 2017, although the figures are not directly comparable (see p19).

The finance industry is responding by:

- 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.
- Working with consumer groups as part of the Payment Systems Regulator's Steering Group to develop an industry code for the reimbursement of victims of authorised push payment scams.
- Joining with government and law enforcement to deter and disrupt the criminals responsible and better trace, freeze and return stolen funds.
- Implementing new standards to ensure those who have fallen victim to fraud or scams get the help they need.
- 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 this year prevented £14.6 million in fraud and led to 100 arrests.
- Sponsoring a specialist police unit, the Dedicated Card and Payment Crime Unit, which tackles the organised criminal groups responsible for financial fraud and scams. In the first half of 2018, the Unit prevented £25m of fraud and carried out 84 arrests and interviews under caution.
- Working with the Information Commissioner's Office to establish guidance on how information about APP scams can be shared between our members, so they can protect their customers, while calling for new powers on information sharing to allow banks to share data to detect and prevent financial crime better.
- 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.

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

- A genuine bank or organisation will never contact you out of the blue to ask for your PIN, full password or to move money to another account. 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.
- 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.
- Always question uninvited approaches in case it's a scam. Instead, contact the company directly using a known email or phone number.

# Unauthorised fraudulent transactions: January to June 2018

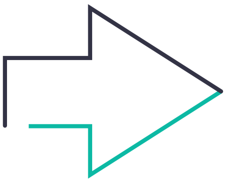
| Overall unauthorised fraud | H1 2014 | H2 2014 | H1 2015 | H2 2015 | H1 2016 | H2 2016 | H1 2017 | H2 2017 | H1 2018 | H1 17/H1 18 % |
|---|---|---|---|---|---|---|---|---|---|---|
| Prevented Value | N/A | N/A | £939.5m | £821.5m | £678.7m | £708.9m | £751.4m | £706.8m | £705.7m | -6% |
| Total losses | £306.9m | £290.6m | £320.3m | £435.3m | £400.4m | £368.4m | £365.8m | £365.5m | £358.0m | -2% |
| Total cases | 687,080 | 631,119 | 610,225 | 816,019 | 937,274 | 920,232 | 936,699 | 973,308 | 1,036,367 | 10% |

Losses due to unauthorised transactions on payment cards, remote banking and cheques totalled £358.0 million in the first half of 2018, a decrease of 2 per cent compared to the same period in 2017.

There were 1,036,367 cases of unauthorised financial fraud during January to June 2018, a rise of 10 per cent compared with the year before.

Prevented fraud totalled £705.7 million in the first half of 2018. This represents incidents that were detected and prevented by banks and card companies and is equivalent to £6.63 in every £10 of attempted fraud being stopped. The proportion of prevented fraud has decreased from £6.72 in every £10 in the first half of 2017.

# Authorised push payment scams: January to June 2018



| Overall authorised push payment scams | H1 2017 | H1 2018 | H1 17/H1 18 % |
|---|---|---|---|
| Total number of cases | 19,370 | 34,128 | 76% |
| Total case value | £101.2m | £145.4m | 44% |
| Total returned to the customer | £26.1m | £30.9m | 18% |

Total losses due to authorised push payment (APP) scams were £145.4 million in the first half of 2018, an increase of 44 per cent compared to the same period in 2017, although the figures are not directly comparable as:

Four additional UK Finance members began reporting APP data to us as of January 2018.

In January 2018, UK Finance introduced new Best Practice Standards for banks and building societies responding to APP scam claims, greatly improving the identification and reporting processes.. Financial providers were able to return £30.9 million of the losses.

There were 34,128 cases of authorised push payment scams.

# What's driving the fraud losses?

Criminals use a wide range of tactics to commit fraud. While it is not possible to attribute the values to individual methods, intelligence reported by our members highlights the main drivers.

Social engineering, in which criminals groom and manipulate people into divulging personal or financial details or transferring money, continued to be the key driver of both unauthorised and authorised fraud losses in the first half of 2018.

A common form of social engineering is an impersonation and deception 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.

To facilitate unauthorised fraud, criminals use impersonation scams to trick their intended victims into giving away their personal or financial information, such as passwords and passcodes, card and bank account details, or into allowing remote access to their computer. The scammers often claim there has been suspicious activity on a bank or card account, account details need to be 'updated' or 'verified', or a refund is due.

Criminals also use impersonation and deception scams to trick their victims into authorising a payment to them. Fraudsters use a wide variety of tactics to commit this crime. These include impersonating a bank staff member or a police officer and claiming fraud has been identified and that money needs to be transferred to a 'safe account'; sending fake invoices to businesses; and offering fraudulent investment.

Data theft also continues to be a major enabler of fraud and contributor to fraud losses. This occurs particularly through third-party data breaches, but also includes mail intercepts, malware and phishing. The stolen data is either used by criminals to commit fraud directly, for example card details are used to make an unauthorised purchase online, or personal details are used to apply for a credit card.

Stolen personal and financial information is also used by criminals to target individuals in impersonation and deception scams. This can include contact details, such as email addresses and telephone numbers, being used by the criminal to communicate with their victim, or other personal or financial details which they use to add apparent authenticity to their approach by repeating the details back to the victim.

Intelligence also suggests criminals are using more low-tech methods such as distractions thefts and card entrapments to steal debit and credit cards which are then used to commit unauthorised 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.

For the first time in 2018, UK Finance is reporting enhanced data on authorised push payment (APP) scams.

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.

# Unauthorised debit and credit and other payment card fraud

| Total payment card fraud | H1 2014 | H2 2014 | H1 2015 | H2 2015 | H1 2016 | H2 2016 | H1 2017 | H2 2017 | H1 2018 | H1 17/H1 18 % |
|---|---|---|---|---|---|---|---|---|---|---|
| Prevented value | N/A | N/A | £366.3m | £477.3m | £475.7m | £510.3m | £502.4m | £482.4m | £493.5m | -2% |
| Total losses | £247.6m | £231.4m | £244.6m | £323.5m | £321.5m | £296.5m | £286.7m | £278.8m | £281.2m | -2% |
| Total cases | 671,388 | 616,824 | 593,417 | 793,775 | 917,479 | 903,247 | 916,867 | 956,649 | 1,020,890 | 11% |

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 £281.2 million in the first half of 2018, a decrease of 2 per cent on the same period in 2017.

Over this period, overall value of card spending grew by 3% per cent. Card fraud as a proportion of card purchases has decreased from 7.5p in the first half of 2017 to 7.2p in the first half of 2018.

A total of £493.5 million of card fraud was stopped by banks and card companies in the first six months of 2018, a decrease of 2 per cent on the same period in 2017. This is equivalent to £6.37 in every £10 of attempted card fraud being prevented.

The finance industry is tackling card fraud by:

- Continuously investing in advanced security systems to authenticate customers and identify any suspicious transactions.
- Developing and providing fraud detection tools for retailers, such as 3D Secure authentication technology which protects online card purchases.
- Speedily, safely and securely identifying compromised card details through UK Finance's intelligence hub so that card issuers can put the necessary protections in place.
- Working with government and law enforcement through 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, a specialist police unit which targets the organised criminal groups responsible for card fraud.

## Remote purchase fraud

| Remote purchase fraud | H1 2014 | H2 2014 | H1 2015 | H2 2015 | H1 2016 | H2 2016 | H1 2017 | H2 2017 | H1 2018 | H1 17/H1 18 % |
|---|---|---|---|---|---|---|---|---|---|---|
| Loss value | £174.5m | £157.m | £171.7m | £226.7m | £224.1m | £208.2m | £204.8m | £203.6m | £211.6m | 3% |
| Number of cases | 537,302 | 481,844 | 473,504 | 639,580 | 728,087 | 709,745 | 703,729 | 694,424 | 791,492 | 12% |

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 by 3 per cent to £211.6 million in the first half of 2018. The number of cases rose by 12 per cent, resulting in a lower average case value which suggests 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 £162.6 million in the first half of 2018, an increase of 5% when compared to the same period in 2018.

| Remote purchase fraud: E-commerce/ Mail order telephone order split | H1 2014 | H2 2014 | H1 2015 | H2 2015 | H1 2016 | H2 2016 | H1 2017 | H2 2017 | H1 2018 | H1 17/H1 18 % |
|---|---|---|---|---|---|---|---|---|---|---|
| E-commerce | £118.5m | £100.6m | £107.2m | £154.2m | £156.4m | £152.4m | £154.5m | £155.4m | £162.6m | +5% |
| Mail and telephone order | £56.0m | £56.4m | £64.4m | £72.5m | £67.7m | £55.8m | £51.0m | £48.1m | £49.1m | -4% |

### How to stay safe from this 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.
- Trust your instincts – 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 fraud

| Lost and stolen fraud | H1 2014 | H2 2014 | H1 2015 | H2 2015 | H1 2016 | H2 2016 | H1 2017 | H2 2017 | H1 2018 | H1 17/H1 18 % |
|---|---|---|---|---|---|---|---|---|---|---|
| Loss value | £29.2m | £30.5m | £30.3m | £43.8m | £49.5m | £46.8m | £47.8m | £45.1m | £42.9m | -10% |
| Number of cases | 66,218 | 67,725 | 61,500 | 82,302 | 109,110 | 122,054 | 148,474 | 201,805 | 185,563 | 25% |

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 due to lost and stolen fraud fell by 10 per cent in the first half of 2018 to £42.9 million. The number of incidents increased by 25 per cent during the same period, resulting in a lower average loss value per individual case as bank systems detected fraudulent spending on a lost or stolen card more quickly.

Intelligence reported to UK Finance suggests criminals are continuing to use low-tech methods such as distractions thefts and card entrapments at ATMs to steal debit and credit cards, along with the PIN, which are then used to commit fraud.

### How to stay safe from lost and stolen fraud:

- Always report any lost or stolen cards to your bank or card company straight away.
- Check your statements regularly and if you spot any payments you don't recognise then contact your card company immediately.
- Make sure you fully cover your PIN with your free hand or purse whenever you enter it.
- If you spot anything suspicious with an ATM, or someone is watching you, then do not use the machine and report it to your bank.

## Card not received fraud

| Card not received fraud | H1 2014 | H2 2014 | H1 2015 | H2 2015 | H1 2016 | H2 2016 | H1 2017 | H2 2017 | H1 2018 | H1 17/H1 18 % |
|---|---|---|---|---|---|---|---|---|---|---|
| Loss value | £5.0m | £5.0m | £5.7m | £5.9m | £6.1m | £6.4m | £5.6m | £4.6m | £3.1m | -45% |
| Number of cases | 4,366 | 4,936 | 5,033 | 5,686 | 5,685 | 5,692 | 5,466 | 5,437 | 4,244 | -22% |

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

Card not received fraud losses fell by 45 per cent in the first half of 2017 to £3.1 million. Criminals often target multi-occupancy buildings, such as flats, where post is not securely stored, to commit this type of 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

| Counterfeit card fraud | H1 2014 | H2 2014 | H1 2015 | H2 2015 | H1 2016 | H2 2016 | H1 2017 | H2 2017 | H1 2018 | H1 17/H1 18 % |
|---|---|---|---|---|---|---|---|---|---|---|
| Loss value | £24.1m | £23.7m | £19.8m | £25.9m | £21.3m | £15.7m | £12.7m | £11.5m | £7.7m | -39% |
| Number of cases | 49,924 | 49,355 | 39,711 | 46,310 | 58,268 | 50,329 | 43,426 | 41,599 | 24,524 | -44% |

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.

Counterfeit card fraud losses fell by 39 per cent to £7.7 million in the first half of 2018. This is the lowest ever half year total for counterfeit card fraud and 91 per cent lower than in 2008, when it totalled £88.8 million. This is likely due to the rollout of chip technology across the world, particularly recently in the United States.

### How to stay safe from counterfeit card fraud:

- Always protect your PIN by fully covering the keypad with your free hand 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

| Card ID theft | H1 2014 | H2 2014 | H1 2015 | H2 2015 | H1 2016 | H2 2016 | H1 2017 | H2 2017 | H1 2018 | H1 17/H1 18 % |
|---|---|---|---|---|---|---|---|---|---|---|
| Loss value | £14.7m | £15.2m | £17.1m | £21.1m | £20.5m | £19.5m | £15.7m | £14.1m | £15.9m | 1% |
| Number of cases | 13,578 | 12,964 | 13,669 | 19,897 | 16,329 | 15,427 | 15,772 | 13,384 | 15,067 | -4% |

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

In a third-party application fraud, a criminal uses stolen or fake documents to open a card account in someone else's name. This information will have likely 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.

Third party application fraud accounted for £8.1 million of card ID theft during the first six months of 2018, up 44 per cent from £5.6 million in the same period in 2017. Account take-over fraud accounted for £7.8 million of card ID theft, down 23 per cent from £10.1 million in 2016.

### 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.
- 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.

# Further card fraud analysis

Figures in the following sections relate to the places where the card was fraudulently used, rather than how the card or card details were compromised.

These figures provide a different breakdown of the overall payment card fraud totals and are not in addition to those in the previous sections. Case volumes are not available for the place of misuse 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

| UK retail face-to-face card fraud | H1 2014 | H2 2014 | H1 2015 | H2 2015 | H1 2016 | H2 2016 | H1 2017 | H2 2017 | H1 2018 | H1 17/H1 18 % |
|---|---|---|---|---|---|---|---|---|---|---|
| Loss value | £25.6m | £23.6m | £22.9m | £30.6m | £31.8m | £31.0m | £31.2m | £30.7m | £30.5m | -2% |

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 payments made by both contactless cards and mobile devices. Fraud on contactless cards and devices remains low with £8.4 million of losses during the first half of 2018, compared to spending of £31.9 billion over the same period.

This is equivalent to 2.5p in every £100 spent using contactless technology, the same as it was in the first half of 2017. Fraud on contactless cards and devices represents 3 per cent of overall card fraud. A zero floor limit is now in place on contactless card transactions, meaning that these transactions are now 'online' regardless of the value, so that the transaction is directly authorised by the card issuer.

## UK cash machine fraud

| UK cash machine fraud | H1 2014 | H2 2014 | H1 2015 | H2 2015 | H1 2016 | H2 2016 | H1 2017 | H2 2017 | H1 2018 | H1 17/H1 18 % |
|---|---|---|---|---|---|---|---|---|---|---|
| Loss value | £14.3m | £13.0m | £14.9m | £17.8m | £20.6m | £22.5m | £20.5m | £16.7m | £15.1m | -27% |

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

Losses at UK cash machines fell 27 per cent to £15.1 million in the first half of 2018.

Intelligence suggests much of this fraud is due to distraction thefts and card entrapment at ATMs, shops and bars, with fraudsters obtaining both the card and the PIN which enables them to make fraudulent cash withdrawals.

## Domestic and international card fraud

| Domestic / International split | H1 2014 | H2 2014 | H1 2015 | H2 2015 | H1 2016 | H2 2016 | H1 2017 | H2 2017 | H1 2018 | H1 17/H1 18 % |
|---|---|---|---|---|---|---|---|---|---|---|
| UK fraud | £175.1m | £153.6m | £164.6m | £215.1m | £215.2m | £202.7m | £204.9m | £202.5m | £207.3m | 1% |
| International fraud | £72.5m | £77.8m | £80.1m | £108.4m | £106.3m | £93.9m | £81.7m | £76.2m | £73.9m | -10% |

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.

Intelligence suggests that much of the decline in international fraud is due to the roll out of Chip & PIN technology around the world.

# Unauthorised remote banking fraud

| Total remote banking fraud | H1 2014 | H2 2014 | H1 2015 | H2 2015 | H1 2016 | H2 2016 | H1 2017 | H2 2017 | H1 2018 | H1 17/H1 18 % |
|---|---|---|---|---|---|---|---|---|---|---|
| Prevented value | N/A | N/A | £311.3m | £213.3m | £103.2m | £102.2m | £160.2m | £100.9m | £137.8m | -14% |
| Total losses | £47.3m | £51.0m | £66.2m | £102.4m | £71.5m | £65.6m | £73.8m | £82.3m | £73.6m | 0% |
| Total cases | 10,908 | 10,911 | 13,971 | 19,335 | 17,687 | 15,705 | 18,848 | 15,898 | 14,780 | -22% |

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.

Remote banking fraud totalled £73.6 million in the first half of 2018, flat compared to the same period in 2017.

A total of £137.8 million of attempted remote banking fraud was stopped by bank security systems during the first half of the year. This is equivalent to £6.52 in every £10 of fraud attempted being prevented.

The proportion of prevented fraud has fallen from £6.85 in every £10 during the same period in 2017.

In addition, 24 per cent (£17.8 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 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 on how they can protect themselves from fraud and scams.
- 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

| Internet banking fraud | H1 2014 | H2 2014 | H1 2015 | H2 2015 | H1 2016 | H2 2016 | H1 2017 | H2 2017 | H1 2018 | H1 17/H1 18 % |
|---|---|---|---|---|---|---|---|---|---|---|
| Loss value | £39.9m | £41.6m | £50.4m | £83.1m | £56.1m | £45.6m | £55.5m | £65.7m | £56.7m | 2% |
| Number of cases | 8,150 | 7,891 | 8,417 | 11,274 | 11,195 | 8,893 | 11,725 | 10,020 | 9,548 | -19% |

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 due to internet banking fraud rose by 2 per cent in the first half of 2017 to £56.7 million, while the number of cases decreased by 19 per cent to 9,548.

£15.5 million (27 per cent) of these losses were recovered after the incident.

Intelligence suggests the rise in the value of the average individual case of internet banking fraud is as a result of criminals targeting business bank accounts, where the average value of a transaction is typically larger.

To commit this fraud, criminals are using social engineering tactics to trick customers into revealing their online banking security details through scam phone calls, texts and emails. These details are then used to access a customer's online account and to make an unauthorised transaction.

### 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

| Telephone banking fraud | H1 2014 | H2 2014 | H1 2015 | H2 2015 | H1 2016 | H2 2016 | H1 2017 | H2 2017 | H1 2018 | H1 17/H1 18 % |
|---|---|---|---|---|---|---|---|---|---|---|
| Loss value | £7.4m | £9.4m | £14.7m | £17.6m | £13.1m | £16.5m | £15.6m | £12.7m | £12.9m | -17% |
| Number of cases | 2,758 | 3,020 | 4,777 | 6,603 | 4,949 | 5,546 | 5,273 | 4,304 | 3,932 | -25% |

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 17 per cent to £12.9 million in the first half of 2018.

In addition, £2.7 million (21 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

| Mobile banking fraud | H1 2014 | H2 2014 | H1 2015 | H2 2015 | H1 2016 | H2 2016 | H1 2017 | H2 2017 | H1 2018 | H1 17/H1 18 % |
|---|---|---|---|---|---|---|---|---|---|---|
| Loss value | N/A | N/A | £1.0m | £1.8m | £2.2m | £3.5m | £2.6m | £3.9m | £4.0m | 54% |
| Number of cases | N/A | N/A | 777 | 1,458 | 1,543 | 1,266 | 1,850 | 1,574 | 1,300 | -30% |

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

Losses due to mobile banking fraud totalled £4 million in the first half of 2017, a 54 per cent rise on the same period in 2017. This rise reflects the growing number of customers using mobile banking and a larger offering of mobile banking facilities by banks.

£1.5 million (38 per cent) of these losses across mobile banking were recovered after the incident.

### How to stay safe from mobile banking fraud:

- Don't be tricked into giving a fraudster access to your personal or security details. Never automatically click on a link in an unexpected email or text and always question uninvited approaches.
- Be wary of text messages that encourage you urgently to visit a website or call a number to verify or update your details.
- Always question uninvited approaches in case it's a scam. Instead, contact the company directly using a known email or phone number.

# Cheque fraud

| Total cheque fraud | H1 2014 | H2 2014 | H1 2015 | H2 2015 | H1 2016 | H2 2016 | H1 2017 | H2 2017 | H1 2018 | H1 17/H1 18 % |
|---|---|---|---|---|---|---|---|---|---|---|
| Prevented value | £212.1m | £216.8m | £262.0m | £130.9m | £99.8m | £96.4m | £88.8m | £123.5m | £74.3m | -16% |
| Total losses | £12.0m | £8.2m | £9.5m | £9.4m | £7.4m | £6.3m | £5.4m | £4.4m | £3.2m | -41% |
| Total cases | 4,784 | 3,384 | 2,837 | 2,909 | 2,108 | 1,280 | 984 | 761 | 697 | -29% |

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.

Cheque fraud losses fell to £3.2 million in the first half of 2018, a 41 per cent drop compared to the same period in 2017. This is the lowest half-year total ever reported.

A total of £74.3 million of cheque fraud was prevented by in the first half of 2018. This is equivalent to £9.59 in every £10 of attempted cheque fraud being stopped before a loss occurs.

## 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.
- Check your statements regularly and if you spot any payments you don't recognise then contact your bank immediately.

# Authorised push payment 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.

While the data for the first half of 2017 is included in the following tables, it is not directly comparable to the 2018 data as:

Four additional UK Finance members began reporting APP data to us as of January 2018.

In January 2018, UK Finance introduced new Best Practice Standards for banks and building societies responding to APP scam claims, greatly improving the identification and reporting processes.

| Authorised push payment scams | | Personal | | | Non-personal | | | Total | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | H1 2017 | H1 2018 | H1 17/H1 18 % | H1 2017 | H1 2018 | H1 17/H1 18 % | H1 2017 | H1 2018 | H1 17/H1 18 % |
| Volume | Number of cases | 16,810 | 31,510 | 87% | 2,560 | 2,618 | 2% | 19,370 | 34,128 | 76% |
| | Number of payments | N/A | 47,346 | N/A | N/A | 3,620 | N/A | N/A | 50,966 | N/A |
| Value | Total case value | £46.9m | £92.9m | 98% | £54.3m | £52.5m | -3% | £101.2m | £145.4m | 44% |
| | Total subsequently returned to the customer | £9.6m | £15.4m | 61% | £16.5m | £15.5m | -6% | £26.1m | £30.9m | 18% |

Losses due to authorised push payment (APP) scams totalled £145.4 million in the first half of 2018. This was split between personal (£92.9 million) and non-personal or business (£52.5 million).

In total there were 34,128 cases of authorised push payment fraud in the first six months of 2018. Of this total, 31,510 cases were on personal accounts and 2,618 cases were on non-personal accounts.

One case can include several payments and there was a total of 50,966 during the period.

Financial providers were able to return a total of £30.9 million of the losses in the first half of 2018.

In an authorised push payment scam a criminal tricks their victim into sending money directly from their account to an account which the criminal controls. Criminals use a range of social engineering tactics to commit this crime. Typically, this includes the criminal posing as genuine individual or organisation and contacting the victim using a range of methods including via the telephone, email and text message. Intelligence suggests that criminals are increasingly using social media to carry out an APP scam.

Once the victim has authorised the payment and the money arrives 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.

If a customer authorises the payment themselves, current legislation means that they have no legal protection to cover them for losses – which is different for an unauthorised transaction.

### 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, in conjunction with the Home Office.
- Working with consumer groups as part of the Payment Systems Regulator's Steering Group to develop an industry code for the reimbursement of victims of authorised push payment scams.
- Implementing new 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 this year prevented £14.6 million in fraud and led to 100 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.
- Working with the Information Commissioner's Office to establish guidance on how information about APP scams can be shared between our members, so they can protect their customers.
- 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.

# Further analysis of the APP scam data

From January 2018, UK Finance has collated 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), Intra-bank ("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 these total figures.

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

# Scam types

## Purchase scams

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 the 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 the most common form of APP scam, accounting for 63 per cent of the total number of APP scam cases. The lower average case value means that they accounted for 13 per cent of the total value of APP scams.

| Purchase scams | H1 2018 |
|---|---|
| Number of cases | 21,483 |
| Number of payments | 27,011 |
| Total value of losses | £19.4m |
| Total subsequently returned to the customer | £1.6m |

### 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.
- Always do your research and ask questions before you buy. Ask to see any vehicle in person first and request the relevant documentation to ensure the seller owns it.
- If you're buying an item made by a major brand, you can often find a list of authorised sellers on their official website.
- Contact your bank straight away if you think you may have fallen victim to a purchase scam.

## Investment scams

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.

Investment scams accounted for only 4 per cent of the total number of APP scam cases, but 14 per cent of the total value.

| Investment scams | H1 2018 |
|---|---|
| Number of cases | 1,359 |
| Number of payments | 3,675 |
| Total value of losses | £20.9m |
| Total subsequently returned to the customer | £1.4m |

### 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.
- Watch out for any too good to be true investment opportunities. If you are being pressurised to invest quickly it is 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

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 2 per cent of the total number of APP scam cases in the first six months of 2018 and 4 per cent of the total value.

| Romance scams | H1 2018 |
|---|---|
| Number of cases | 571 |
| Number of payments | 3,372 |
| Total value of losses | £5.3m |
| Total subsequently returned to the customer | £0.3m |

### 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

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 second most common form of APP scam in the first half of 2018, accounting for 11 per cent of the total number of cases. However, by value these scams accounted for 4 per cent.

| Advance fee scams | H1 2018 |
|---|---|
| Number of cases | 3,646 |
| Number of payments | 6,045 |
| Total value of losses | £6.0m |
| Total subsequently returned to the customer | £0.5m |

### 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 or would need to pay in advance to claim any winnings.
- Contact your bank straight away if you think you may have fallen victim to an advance fee scam.

## Invoice and Mandate scams

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 third most common type of APP scam, however it resulted in the largest share of losses at 34 per cent. The majority of losses by value were from non-personal or business accounts.

| Invoice and mandate scams | H1 2018 |
|---|---|
| Number of cases | 2,856 |
| Number of payments | 3,705 |
| Total value of losses | £49.3m |
| Total subsequently returned to the customer | £13.3m |

### How to stay safe from invoice and mandate scams:

Always confirm any bank account details directly with the company either on the telephone or in person before you make a payment or transfer any money.

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

## CEO Fraud

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 2018, accounting for 1 per cent of total cases. It accounted for 6 per cent of total losses.

| CEO fraud | H1 2018 |
|---|---|
| Number of cases | 347 |
| Number of payments | 478 |
| Total value of losses | £8.0m |
| Total subsequently returned to the customer | £2.2m |

### 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 an email or letter.
- Establish documented internal processes for requesting and authorising all payments and be suspicious of any request to make a payment outside of the company's standard process.
- Be cautious about any unexpected emails or letters which request urgent bank transfers, even if the message appears to have originated from someone from your own organisation.
- Contact your bank straight away if you think you may have fallen victim to CEO fraud.

## Impersonation: Police/Bank Staff

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 6 per cent of all APP scam cases in the first half of 2018. However, by value this scam was the second highest, accounting for 15 per cent of total losses.

| Impersonation: Police/Bank Staff | H1 2018 |
|---|---|
| Number of cases | 1,947 |
| Number of payments | 3,196 |
| Total value of losses | £22.2m |
| Total subsequently returned to the customer | £6.9m |

### 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 victim to an impersonation scam.

## Impersonation: Other

In this scam, a criminal 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 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.

6 per cent of all APP scam cases were due to this type of scam in the first half of 2017, accounting for 10 per cent of total losses.

| Impersonation: Other | H1 2018 |
|---|---|
| Number of cases | 1,919 |
| Number of payments | 3,484 |
| Total value of losses | £14.4m |
| Total subsequently returned to the customer | £4.8m |

### How to stay safe from impersonation scams:

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

## Payment type

| Payment type | Number of cases<br>H1 2018 | Value of cases<br>H1 2018 |
|---|---|---|
| Faster Payment | 47,520 | £99.3m |
| CHAPS | 355 | £13.3m |
| BACS: Payment | 568 | £9.5m |
| BACS: Standing Order | 29 | £0.0m |
| Intra Bank Transfer ('on us') | 921 | £2.0m |
| International | 1,573 | £21.2m |
| Total | 50,966 | £145.4m |

This data shows the type of payment method the victim used to make the authorised push payment. Faster Payment was used in 93 per cent of cases.

## Payment channel

| Payment type | Number of cases<br>H1 2018 | Value of cases<br>H1 2018 |
|---|---|---|
| Branch | 3,344 | £18.9m |
| Internet Banking | 39,157 | £117.2m |
| Telephone Banking | 2,275 | £6.1m |
| Mobile Banking | 6,190 | £3.1m |
| Total | 50,966 | £145.4m |

This data shows the channel through which the victim made the authorised push payment. Internet banking was used in 77 per cent of cases.