Financial Fraud Action UK
Working together to prevent fraud

UK FINANCE

2017 annual fraud update:

Payment cards, remote banking, cheque and authorised push payment scams

March 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, remote banking and cheques, and, as of 2017, authorised push payment scams (also known as APP or authorised bank transfer scams).

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

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

In 2017, losses due to unauthorised financial fraud on payment cards, remote banking and cheques fell by 5 per cent to £731.8 million.

In 2017, a total of £236.0 million was lost due to authorised push payment scams. This is the first time an annual figure has been collated.

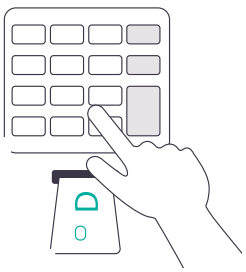
To stay safe, customers are urged to follow the advice of our Take Five campaign:

- 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.

The finance industry is responding 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 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.
- Implementing new standards to ensure those who have fallen victim to fraud or scams get the help they need, including around-the-clock availability of fraud specialists in every bank, to make it easier and better for the customer, and, where possible, improve the likelihood of their funds being recovered.
- 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.
- Rolling out the Banking Protocol – a ground-breaking rapid response scheme through which branch staff can alert police and Trading Standards to suspected frauds taking place – to every police force area in the UK. In 2017, while it was still being introduced across the country, the Protocol prevented £13.3 million of fraud and led to 129 arrests.
- Sponsoring the Dedicated Card and Payment Crime Unit (DCPCU), a specialist police unit which tackles the organised criminal groups responsible for financial fraud and scams. This has led to a combined value in savings and disruptions in criminal activity of close to £30 million in 2017.
- Exploring new ways to track stolen funds moved between multiple bank accounts.

Unauthorised fraudulent transactions: January to December 2017



Unauthorised fraud losses	2012	2013	2014	2015	2016	2017	16/17 %
Prevented	N/A	N/A	N/A	£1761.0mn	£1387.5mn	£1458.6mn	5%
Gross Losses	£499.8mn	£553.3mn	£597.5mn	£755.6mn	£768.8mn	£731.8mn	-5%
Gross Cases	1,036,496	1,261,783	1,318,199	1,426,244	1,857,506	1,910,490	3%

Losses due to unauthorised transactions on payment cards, remote banking and cheques totalled £731.8 million in 2017, a decrease of 5 per cent compared to 2016.

- There were 1,910,490 cases of unauthorised financial fraud during 2017, a rise of 3 per cent compared with the year before.
- Prevented fraud totalled £1458.6 million in 2017. This represents incidents that were detected and prevented by banks and card companies and is equivalent to £2 in every £3 of attempted fraud being stopped.

Authorised push payment scams: January to December 2017

Authorised losses	Total
Total cases	43,875
Total victims	42,837
Total value	£236.0mn
Total returned to victim	£60.8mn

Total losses due to authorised push payment scams were £236.0 million. Financial providers were able to return £60.8 million of the losses 2017.

There were 43,875 cases of authorised push payment scams, with 42,837 victims.

What's driving the fraud losses?

Fraudsters use a wide range of tactics. While it is not possible to be more specific about the values that can be attributed to individual methods, intelligence from our members highlights the main drivers.

In 2017, criminals' use of social engineering tactics through deception and impersonation scams continues to be a key driver of both unauthorised and authorised fraud losses. Social engineering is a method through which criminals manipulate people into divulging personal or financial details, or into transferring money directly to the them. In an impersonation scam, fraudsters contact customers by phone, text message or email pretending to represent a trusted organisation, such as a bank, the police, a utility company or a government department.

Often the approach claims there has been suspicious activity on an account, account details need to be 'updated' or 'verified', or a refund is due. The criminal then attempts to trick their intended victim 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. This information is then used by the criminal to make an unauthorised payment.

Criminals also use these fraudulent approaches to trick them into authorising a payment to them. Fraudsters use a range of tactics to commit this crime, including impersonating someone from a bank or a police officer, claiming a fraud has been spotted on a customer's account and that money needs to be transferred to a 'safe account'; sending fake invoices to businesses; offering fraudulent investment opportunities; and online auction scams.

Data breaches also continue to be a major contributor to fraud losses. Criminals use stolen data to commit fraud directly, for example card details are used to make unauthorised purchases online or personal details used to apply for credit cards. Stolen personal and financial information is also used by criminals to target individuals in impersonation and deception scams, and can add apparent authenticity to their approach.

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 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.

Debit and credit and other payment card fraud

Total UK issued payment card fraud	2012	2013	2014	2015	2016	2017	16/17 %
Prevented value	N/A	N/A	N/A	£843.5mn	£986.0mn	£984.9mn	0%
Total losses	£390.4mn	£450.2mn	£479.0mn	£568.1mn	£618.1mn	£566.0mn	-8%
Total cases	997,507	1,231,917	1,288,212	1,387,192	1,820,726	1,874,002	3%

Total UK-issued payment card fraud

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 £566.0 million in 2017, a decrease of 8 per cent on 2016.

Over this period, overall value of card spending grew by 7 per cent. Card fraud as a proportion of card purchases has decreased from 8.3p at the end of 2016 to 7.0p at the end of 2017; the lowest reported since 2012 (6.9p)

A total of £984.9 million of card fraud was stopped by banks and card companies in 2017, static when compared to 2016. This is equivalent to £6.66 in every £10 of attempted card fraud being prevented.

The finance industry is tackling card fraud by:

- Investing in new, innovative security tools to identify suspicious transactions, including even more sophisticated ways of authenticating customers.
- Providing fraud screening detection tools for retailers, such as the continued development of 3D Secure technology which protects card purchases online.
- Speedily, safely and securely identifying compromised card details through UK Finance's intelligence hub so that card issuers can put protections in place.
- Working with government and law enforcement in the Joint Fraud Taskforce to use our collective powers, systems and resources to crack down on financial fraud.
- Fully-sponsoring a specialist police unit, the Dedicated Card and Payment Crime Unit, which targets organised criminals groups responsible for card fraud

Remote purchase fraud

Remote purchase fraud	2012	2013	2014	2015	2016	2017	16/17 %
Loss value	£247.3mn	£301.0mn	£331.5mn	£398.4mn	£432.3mn	£409.4mn	-5%
Number of cases	752,450	951,998	1,019,146	1,113,084	1,437,832	1,399,031	-3%

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 fell by 5 per cent to £409.4 million in 2017.

Intelligence suggests remote purchase fraud continues to result mainly from criminals using card details stolen through data hacks, via phishing emails, and scam text messages.

Contained within these figures, e-commerce card fraud totalled an estimated £310.2 million in 2017, static when compared to 2016.

Remote purchase fraud: E-commerce/ Mail order tele-phone order split	2012	2013	2014	2015	2016	2017	16/17 %
E-commerce	£140.2m	£190.1m	£219.1m	£261.5m	£310.3m	£310.2m	0%
Mail and telephone order	£107.1m	£111.0m	£112.4m	£136.7m	£122.0m	£99.1m	-19%

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.
- Look for the padlock symbol in the web address bar. It's a good indication that a retailer is reputable.
- 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.

Lost and stolen fraud

Lost and stolen fraud	2012	2013	2014	2015	2016	2017	16/17 %
Loss value	£55.4mn	£58.9mn	£59.7mn	£74.1mn	£96.3mn	£92.5mn	-4%
Number of cases	113,162	138,967	133,943	143,802	231,164	350,066	51%

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.

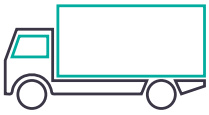
Losses due to lost and stolen fraud fell by 4 per cent in 2017 to £92.5 million. The number of incidents increased by 51 per cent, indicating a lower loss value per individual case as bank systems detected fraudulent spending on a lost or stolen card more quickly.

Intelligence suggests criminals are using more low-tech methods such as distractions thefts and card entrapments 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.
- 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.
- Check your statements regularly and if you spot any payments you don't recognise then contact your card company immediately.

Card not received fraud



Card not received fraud	2012	2013	2014	2015	2016	2017	16/17 %
Loss value	£12.8mn	£10.4mn	£10.1mn	£11.7mn	£12.5mn	£10.1mn	-19%
Number of cases	9,053	9,125	9,302	10,719	11,377	10,905	-4%

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

Card not received fraud losses fell by 19 per cent in 2017 to £10.1 million. To commit this fraud, criminals often target multi-occupancy buildings, such as flats, where post is not securely stored.

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	2012	2013	2014	2015	2016	2017	16/17 %
Loss value	£42.3mn	£43.3mn	£47.8mn	£45.7mn	£36.9mn	£24.2mn	-35%
Number of cases	98,555	101,109	99,279	86,021	108,597	84,861	-22%

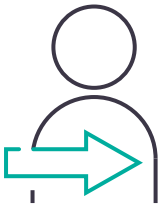
This fraud occurs when a fake card is created by a fraudster using compromised details from the magnetic stripe of a genuine card. This typically occurs because of criminals using a device to steal details from a UK-issued card at an ATM or unattended payment terminal, such as at a car park. A fake magnetic stripe card is then created to be used overseas in countries yet to upgrade to chip & PIN.

Counterfeit card fraud losses fell by 35 per cent to £24.2 million in 2017. This is the lowest ever total for counterfeit card fraud and 86 per cent lower than the peak in 2008, when it totalled £169.8 million. This fall is likely due to the increased rollout of chip technology around the world, particularly in the US.

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 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	2012	2013	2014	2015	2016	2017	16/17 %
Loss value	£32.6mn	£36.7mn	£30.0mn	£38.2mn	£40.0mn	£29.9mn	-25%
Number of cases	24,287	30,718	26,542	33,566	31,756	29,139	-8%

Card ID theft occurs in two ways, through third-party applications or account takeover.

Third-party application fraud happens when a criminal uses stolen or fake documents to open an account in someone else's name. This information will have likely been gathered through data compromise, such as via data hacks and social engineering.

Account takeover occurs when a criminal takes over another person's genuine card account. The criminal will gather information about the intended victim, often through impersonation scams, before contacting the bank or card issuer masquerading as the genuine cardholder.

Third party applications accounted for £11.3 million of card ID theft during 2017, down 28 per cent from £15.6 million in 2016. Account take-over accounted for £18.5 million of card ID theft, down 24 per cent from £24.4 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 rip up 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 are another way of breaking down the overall payment card fraud totals and are not in addition to those covered previously. 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	2012	2013	2014	2015	2016	2017	16/17 %
Loss value	£55.0mn	£57.1mn	£49.4mn	£53.6mn	£62.8mn	£61.8m	-2%

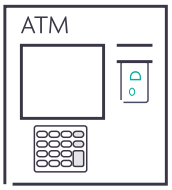
UK retail face-to-face fraud covers all transactions that occur in person in a UK shop.

Most of this fraud takes place using cards obtained through more basic techniques, with fraudsters finding ways of stealing both the card and PIN to carry out fraudulent transactions in shops. This includes criminals targeting cards and PINs through distraction thefts and entrapment devices at ATMs combined with shoulder surfing or PIN pad cameras. Criminals also use methods to dupe victims into handing over their cards on their own doorstep.

Contactless fraud covers fraud on both contactless cards and mobile devices. Fraud on contactless cards and devices remains low with £14 million of losses during 2017, compared to spending of £52.4 billion over the same period.

This is equivalent to 2.7p in every £100 spent using contactless technology, the same as it was in 2016. Fraud on contactless cards and devices represents just 2.5 per cent of overall card fraud losses, while 31 per cent of all card transactions were contactless last year.

UK cash machine fraud



UK cash machine fraud	2012	2013	2014	2015	2016	2017	16/17 %
Loss value	£29.0mn	£31.9mn	£27.3mn	£32.7mn	£43.1mn	£37.2mn	-14%

These figures show how much fraud took place at cash machines in the UK using a compromised card. In all cases the fraudster would need to have access to the genuine PIN and card.

Losses at UK cash machines fell 14 per cent to £37.2 million in 2017.

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	2012	2013	2014	2015	2016	2017	16/17 %
UK fraud	£288.4mn	£328.3mn	£328.7mn	£379.7mn	£417.9mn	£407.6mn	-2%
Overseas	£102.0mn	£122.0mn	£150.3mn	£188.4mn	£200.2mn	£158.4mn	-21%

These figures provide a breakdown of fraud committed on a UK issued credit, debit or charge card split between UK or international fraud spending location.

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

Remote banking fraud

Total remote banking fraud	2012	2013	2014	2015	2016	2017	16/17 %
Prevented value	N/A	N/A	N/A	£524.6mn	£205.4mn	£261.4mn	27%
Total losses	£71.7mn	£71.9mn	£98.3mn	£168.6mn	£137.0mn	£156.1mn	14%
Total cases	23,450	19,395	21,819	33,306	33,392	34,743	4%

Remote banking fraud losses are collated in three categories: internet, phone and mobile banking. It occurs when the fraudster gains access to an individual's bank account and make an unauthorised transfer of money out of it.

Remote banking fraud totalled £156.1 million in 2017, a 14 per cent rise from £137.0 million in 2016.

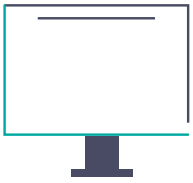
A total of £261.4 million of attempted remote banking fraud was stopped by bank security systems during the first half of the year. This is equivalent to £6.26 in every £10 of fraud attempted being prevented. The proportion of prevented fraud has risen from £6.00 in every £10 during the same period in 2016.

In addition, 25 per cent (£38.7 million) of the losses across all remote banking channels were recovered after the incident.

The finance industry is tackling remote banking fraud by:

- Investing in new, innovative security tools, including ever more sophisticated ways of authenticating customers, such as using biometrics and customer behaviour analysis.
- Providing customers 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 telecommunications industry and other key stakeholders to further improve security and to identify and prosecute the perpetrators.

Internet banking fraud



Internet banking fraud	2012	2013	2014	2015	2016	2017	16/17 %
Loss value	£57.0mn	£58.8mn	£81.4mn	£133.5mn	£101.8mn	£121.4mn	19%
Number of cases	16,355	13,799	16,041	19,691	20,088	21,784	8%

This type of fraud occurs when a fraudster gains access to a customer's online bank account and makes an unauthorised transfer of money from it.

Intelligence suggests fraudsters 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.

Losses due to internet banking fraud rose by 19 per cent in 2017 to £121.4 million, while the number of cases increased by 8 per cent. At the same time, there were in excess of 33 million unique logins into internet banking services during December 2017.

£30.9 million (34 per cent) of these losses were recovered after the incident.

How to stay safe from internet banking fraud:

- A genuine bank or organisation will never contact you out of the blue to ask for your PIN or full password. Only give out your personal or financial details to use a service that you have given your consent to, that you trust and that you are expecting to be contacted by.
- Always question uninvited approaches in case it's a scam. Instead, contact the company directly using a known email or phone number.
- Don't be tricked into giving a fraudster access to your personal or financial details. Never automatically click on a link in an unexpected email or text.
- Ensure you have the most up-to-date security software installed on your computer, including anti-virus. Some banks offer free security software so check your bank's website for details.

Telephone banking fraud

Telephone banking fraud	2012	2013	2014	2015	2016	2017	16/17 %
Loss value	£14.7mn	£13.1mn	£16.8mn	£32.3mn	£29.6mn	£28.4mn	-4%
Number of cases	7,095	5,596	5,778	11,380	10,495	9,575	-9%

Telephone banking fraud occurs when a fraudster gains access to a customer's phone banking account and makes an unauthorised transfer of money from it.

Losses due to telephone banking fraud fell by 4 per cent to £28.4 million in 2017.

In addition, £6.2million (22 per cent) of the losses were recovered after the incident.

How to stay safe from phone 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 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	2012	2013	2014	2015	2016	2017	16/17 %
Loss value	N/A	N/A	N/A	£2.8mn	£5.7mn	£6.3mn	10%
Number of cases	N/A	N/A	N/A	2,235	2,809	3,384	20%

Mobile banking fraud covers fraudulent payments or attempts made via mobile banking services accessed only through a banking app downloaded to a mobile device. It also includes any frauds made via an SMS payment but excludes mobile web browser banking and browser based banking apps.

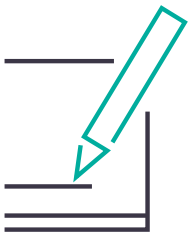
Losses due to mobile banking fraud totalled £6.3 million in 2017, a 10 per cent rise on 2016. The rise in fraud reflects the growing number of customers using mobile banking and a larger offering of mobile banking facilities by banks.

£1.6 million (25 per cent) of these losses across mobile banking were recovered after the incident.

How to stay safe from mobile banking fraud:

- Don't be tricked into giving a fraudster access to your personal or security details. Never automatically click on a link in an unexpected email or text and always question uninvited approaches.
- Be wary of text messages that encourage you urgently to visit a website or call a number to verify or update your details.

Cheque fraud



Total cheque fraud	2012	2013	2014	2015	2016	2017	16/17 %
Prevented value	N/A	N/A	N/A	£392.9mn	£196.2mn	£212.3mn	8%
Total losses	£37.7mn	£31.2mn	£20.3mn	£18.9mn	£13.7mn	£9.8mn	-28%
Total cases	15,539	10,471	8,168	5,746	3,388	1,745	-48%

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.

A fraudulently altered cheque is a genuine cheque that has been made out by the genuine customer, but has been altered in some way by a fraudster before it is paid in, e.g. by changing the beneficiary's name or the amount of the cheque.

Cheque fraud losses fell to £9.8 million in 2017, a 28 per cent drop on 2016. This is the lowest year total ever reported.

A total of £212.3 million of cheque fraud was prevented by bank monitoring systems in 2017. This is equivalent to £9.56 in every £10 of attempted cheque fraud being stopped before a loss occurs.

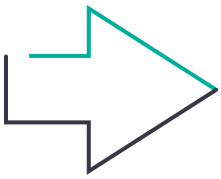
How to stay safe from cheque fraud:

- 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 and always check your bank statement thoroughly.

Some caveats are required for the tables in the document.

- Prevented values were not collected for all fraud types prior to 2015.
- Sum of components may not equal the total due to rounding.

Authorised push payment scams



2017	Personal	Non-Personal	Total
Total cases	38,596	5,279	43,875
Total victims	37,761	5,076	42,837
Total value	£107.5mn	£128.6mn	£236.0mn
Total returned to victim	£22.6mn	£38.2mn	£60.8mn

This is the first time that annual authorised push payment (also known as APP or authorised bank transfer scams) losses have been collated and published.

Losses due to authorised push payment scams totalled £236 million in 2017. This was split between personal (£107.5 million) and non-personal or business (£128.6 million) accounts.

In total there were 43,875 cases of authorised push payment fraud in 2017. 88 per cent of this total were consumers losing an average of £2,784, and the remainder were businesses who lost on average £24,355 per case.

Financial providers were able to return £60.8 million of the losses in 2017.

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.

Intelligence suggests criminals are using a range of social engineering tactics to commit this crime.

These include impersonating someone from a bank or a police officer, claiming a fraud has been spotted on a customer's account and that funds need to be transferred to a 'safe account'; sending fake invoices to businesses; offering fraudulent investment opportunities or through online auction scams.

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.

The finance industry is tackling authorised push payment scams:

- 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 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.
- Implementing new standards to ensure those who have fallen victim to fraud or scams get the help they need, including around-the-clock availability of fraud specialists in every bank, to make it easier and better for the customer, and, where possible, improve the likelihood of their funds being recovered.
- 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.

How to stay safe from authorised push payment scams:

- A genuine bank or organisation will never contact you out of the blue asking you to move money to another account.
- Never give out personal or financial information. Always contact the company directly using a known email or phone number.
- Don't be tricked into giving a fraudster access to your details. Never automatically click on a link in an unexpected email or text.
- Always question uninvited approaches, in case it's a scam.

The Take Five to Stop Fraud campaign was devised by Financial Fraud Action UK to help fight fraud. www.takefive-stopfraud.org.uk

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 External Affairs: info@ukfinance.org.uk