UK FINANCE

FRAUD THE FACTS 2019

The definitive overview of payment industry fraud

UK Finance is the collective voice for the banking and finance industry. Representing more than 250 firms across the industry, it seeks to enhance competitiveness, support customers and facilitate innovation.

The Economic Crime team within UK Finance is responsible for leading the industry's collective fight against economic crime in the UK, including fraud, anti-money laundering (AML), sanctions, anti-bribery, corruption and cybercrime.

UK Finance seeks to ensure that the UK is the safest and most transparent financial centre in the world – working with members, law enforcement, government agencies and industry to create a hostile environment for criminals.

We represent our members by providing an authoritative voice to influence regulatory and political change, both in the UK and internationally. We also act as advocates on behalf of members to both media and customers, articulating the industry's achievements and building its reputation.

We do this by:

- Managing the industry strategic threat management process, which provides an up-to-the-minute picture of the threat landscape.
- Sponsoring the Dedicated Card and Payment Crime Unit (DCPCU), a unique proactive operational police unit with a national remit, formed as a partnership between UK Finance, the City of London Police, and the Metropolitan Police.
- Managing intelligence-sharing through the industry intelligence hub (Financial Fraud Bureau) and the Fraud Intelligence Sharing System (FISS) which feed intelligence to police and other agencies in support of law enforcement activity.
- Providing a single point of contact for companies suffering data breaches, to ensure compromised account information can be speedily, safely and securely repatriated to the banks.
- Delivering UK-wide awareness campaigns (Take Five) to inform customers about threats and how to stay safe Informing commentators and policymakers through our press office and public affairs functions.
- Introducing procedures between police and bank branches to prevent vulnerable people falling victim to fraud (Banking Protocol).
- Providing expert security assessments of new technology, as well as the impact of new legislation and regulation.
- Publishing the official fraud losses for the UK payments industry, as well as acting as the definitive source of industry fraud statistics and data.

CONTENTS

INTRODUCTION

Fraud poses a major threat to the UK. It's a crime that the finance industry is committed to tackling, but it's also one that requires the combined efforts of every sector, both public and private, to overcome.

Our Fraud the Facts 2019 report lays bare the extent of the challenge. Last year the advanced security systems and innovations in which the finance industry invests to protect customers stopped more than £1.6 billion of unauthorised fraud. But despite this, criminals successfully stole £1.2 billion through fraud and scams in 2018.

These crimes can have a devastating impact on victims. And even if the customer gets the money back from their finance provider, the organised criminal gangs which perpetrate these frauds still profit from the proceeds. Money that may go on to fund illicit acts which damage our society – crimes such as terrorism, drug trafficking and people smuggling.

During 2018 the finance industry continued to expand and bolster its defences to protect customers:

- The Banking Protocol – a ground-breaking rapid response scheme through which branch staff can alert police and Trading Standards to suspected frauds taking place – is now operational in every police force area of the UK and prevented customers from losing £38 million of their money to criminals and led to 231 arrests in 2018.
- In November a trial began for a new anti-spoofing system to help root out scam text messages, with the industry working closely with the mobile network operators and service providers. The following month saw the launch of new technology that will help track suspicious payments as they move through the system and identify money mules accounts.
- The Dedicated Card and Payment Crime Unit, the specialist police unit sponsored by the banking industry which tackles the organised criminal groups responsible for financial fraud and scams, prevented £94.5 million of fraud, secured 48 convictions and disrupted 11 organised crime groups last year.
- UK Finance is currently hosting, and part-funding a government-led programme to reform the system of economic crime information sharing, known as Suspicious Activity Reports, so that it meets the needs of crime agencies, regulators, consumers and businesses.

As I write this, following work between the industry, consumer groups and the regulator, a new authorised push payment (APP) scams voluntary code has just been published.

Bringing new protections for consumers, the voluntary code will be implemented on 28 May 2019, with the first group of signatories announced on the same date. The code delivers a significant commitment from all firms who sign up to reimburse victims of authorised push payment scams in any scenario where their bank or payment service provider is at fault and the customer has met the standards expected of them under the code.

But fraud is a threat that the finance industry cannot tackle alone. As this report shows, data breaches at third parties continue to be a major contributor to fraud losses. There has been a number of high-profile incidents in 2018, many targeting well-known brands, where customer data was stolen. Whether it's at a retailer, utility company, transport provider or elsewhere, the theft of personal and financial data can both directly lead to fraud losses or be used by criminals as part of their scams. The data can be used for months and even years after the breach takes place.

These incidents occur outside of the finance industry's control, yet it is banks and their customers who bear the impact. So, it's imperative that any organisation that controls customer data does everything in its power to keep it secure.

There is a moral duty upon us all to act. Every part of society across both the public and private sectors, from online retailers to leisure, travel and social media companies, must work together to beat fraud. The finance industry has a strong track record of combining with government and law enforcement. It's now time for others to join the fight.

KATY WOROBEC
Managing Director: Economic Crime,
UK Finance.

TRENDS AND STATISTICS

2018 overview

Unauthorised financial fraud losses across payment cards, remote banking and cheques totalled £844.8 million in 2018, an increase of 16 per cent compared to 2017.

Banks and card companies prevented £1.66 billion in unauthorised fraud in 2018. This represents incidents that were detected and prevented by firms and is equivalent to £2 in every £3 of attempted fraud being stopped.

In addition to this, in 2018 UK Finance members reported 84,624 incidents of authorised push payment scams with gross losses of £354.3 million.

Authorised fraud: In an authorised 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 authorisation for the payment to proceed and the transaction is carried out by a third party.

Behind the changing fraud figures

Criminals use a wide range of methods to commit fraud. While it is not possible to place specific monetary values on particular tactics criminals use, intelligence reported to UK Finance by our members indicates the key drivers behind the reported figures.

The theft of personal and financial data through social engineering and data breaches was a major contributor to fraud losses in 2018. The stolen data is used to commit fraud both directly and indirectly. For example, compromised card details are used to make unauthorised purchases online and personal details are used to take over an account or apply for a credit card in someone else's name. Criminals also use personal and financial data to defraud customers, using information gained about an individual to add apparent authenticity to a scam.

Social engineering is a tactic by which criminals groom and manipulate people into transferring money or divulging their personal and financial details, with deception scams being a common method. In a deception scam, a criminal will typically pose as a representative from a genuine organisation such as a bank, the police, a retailer, utility company or government department. Fraudsters use a

range of methods to contact customers in deception scams, including by phone, text message, email and social media.

To persuade people to act, the criminal often claims that there has been suspicious activity on an account, that a refund is owed or that account details need to be 'updated' or 'verified' and the customer must act quickly. The criminal's aim is then to trick their intended victim into giving away their personal or financial information, such as security login details and card and bank account information, or into allowing remote access to their computer. This stolen information is then used by the criminal to access an account and make an unauthorised payment.

Deception scams are also used by criminals to persuade people into authorising a payment to them. These include criminals impersonating a member of bank staff or a police officer and claiming there has been fraudulent activity on an account and that money needs to be transferred to a 'safe account'; impersonating a supplier and sending a fake invoice to a business; online auction and sales scams; and investment scams. Criminals use a range of communication methods to deceive their victims, including phone calls and emails. Intelligence also points towards criminals increasingly using social media sites to entice victims with posts advertising items for sale and investments, both of which are fake.

The number of phishing websites targeted against UK banks and building societies has fallen to the lowest level ever this year. Intelligence suggests that criminals are instead increasingly impersonating other organisations such as online retailers, travel and leisure firms, HMRC and telecommunication companies instead.

During 2018 there were a number of significant data breaches which received extensive media coverage, along with a significant volume of smaller-scale breaches. The incidents include well-known brands whose customer information was compromised as a result of a data breach. They cover a range of sectors and occur outside of the control of the banking industry.

Data breaches involving just three significant brands which occurred during 2018 are reported to have resulted in the attempted compromise of around 6.3 million payment card details. While this does not cover the full extent of data that was stolen during the year, it provides a strong indication of the impact of data breaches. The Information Commissioner's Office reports that during the second quarter of 2018/19, there was a total of 4,056 data security incidents.[1] Information stolen through a data breach can be used for months or even years after the event.

UK Finance's intelligence hub, the Financial Fraud Bureau (FFB), provides a single point of contact for companies suffering data breaches to ensure compromised account information can be speedily, safely and securely repatriated to the banks.

Criminals are also using more low-tech methods such as distraction thefts and card entrapments to steal physical debit and credit cards, which are then used to commit fraud.

1. https://ico.org.uk/action-weve-taken/data-security-incident-trends

The industry response

The financial industry is committed to tackling fraud and scams. It is responding to the threat by:

- Investing in advanced security systems to protect customers, including real-time transaction analysis, behavioural biometrics on devices and technology to identify the different sound tones that every phone has and the environment that they are in.
- 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 £38 million in fraud and enabled 231 arrests in 2018.
- 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 2018, the Unit prevented an estimated £94.5 million of fraud, secured 48 convictions and disrupted 11 organised crime groups.
- Working with consumer groups to develop a voluntary code to better protect customers and reduce the occurrence of APP fraud. The code was published in February and will become effective for signatory firms on 28 May 2019.
- Working with Pay.UK to implement Mule Insights Tactical Solution (MITS), a new technology that will help track suspicious payments and identify money mule accounts, and Confirmation of Payee, an account name checking service for when a payment is made, that will help to prevent authorised push payment scams.
- 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.
- Working closely with mobile network operators and the messaging industry to trial a new anti-spoofing system to help root out scam text messages.
- 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.
- 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.

New technology

The banking industry is proactively using technology in the fight against fraud. One example is the use of a system – described as a global digital identity tool – which has been adopted by a number of leading banks to help identify and prevent potential fraud.

The system analyses billions of real-time transactions across many countries including the UK, coupled with additional data including device, geographical, behavioural and threat intelligence input. By combining this with historical data, the bank can build a picture of a customer's behaviour so that any unusual and potentially fraudulent activity can be identified and flagged up.

Tracking technology is also powerful when it comes to identifying money mule accounts, where banks can analyse data anomalies to reveal webs of linked accounts generated by mule activity. The Mule Insights Tactical Solution enables the tracking of suspicious payments between bank and building society accounts, even if the money is split between multiple accounts or travels between different institutions.

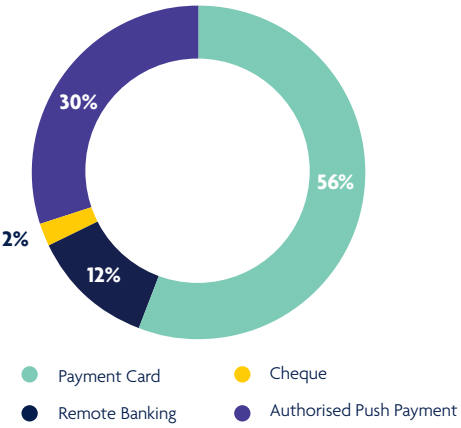
Later this year, new rules will come into force requiring all payment providers to use multi-factor authentication for higher-value and higher-risk transactions. Some card issuers are already beginning to roll out the changes, known as strong customer authentication. The rules mean that when a customer makes certain transactions online, a second level of security would be required, such as a one-time passcode sent via text message or biometrics.

To combat telephone banking fraud, some banks are using technology which allows them to identify the different sound tone that every phone has and the environment that they are in. If someone is calling from an environment which is not their usual one, this can be picked up and investigated further to detect if fraud is being attempted.

Banks are also increasingly looking at 'behavioural biometrics' tools to identify potential cases of fraud and prevent them where possible. Some banks have adopted software that monitors the ways in which consumers type and swipe on their devices or how they hold their device in terms of grip, when logged into banking apps.

If this 'behaviour' changes then the software will flag up potentially suspicious activity and could prompt a call from the bank. Use of this technology has helped to prevent tens of thousands of pounds of fraud going through.

Total 2018 financial fraud losses by type



CARD FRAUD

Unauthorised debit, credit and other payment card fraud

VALUE	£671.4m	19%

VOLUME	2,617,739	40%

Fraud losses on UK-issued cards totalled £671.4 million in 2018, a 19 per cent increase from £565.4 million in 2017. At the same time, total spending on all debit and credit cards reached £800 billion in 2018, with 20.4 billion transactions made during the year.

Overall card fraud losses as a proportion of the amount we spend on our cards increased during 2018, rising from 7p per £100 spent in 2017 to 8.4p per £100 in 2018 (in 2008 it was 12.4p for every £100 spent).

A total of £1.12 billion in card fraud was stopped by banks and card companies in 2018, a rise of 14 per cent on 2017. This is equivalent to £6.27 in every £10 of attempted card fraud being prevented.

These figures cover fraud on debit, credit, charge and ATM only cards issued in the UK. Payment card fraud losses are organised into five categories: remote purchase (card not present or CNP), counterfeit, lost and stolen, card not received and card ID theft.

Victims of unauthorised payment card fraud are legally protected against losses. Industry analysis indicates that banks and card companies refund customers in over 98 per cent of cases.

The finance industry is tackling card fraud by:

- Investing in advanced security systems to protect customers, including real-time transaction analysis and behavioural biometrics on devices. Strong customer authentication for higher value online payments is set to become a legal requirement from September 2019, adding an extra layer of security in the fight against fraud.
- Developing the fraud screening detection tools available for retailers to use, such as 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 criminal groups responsible for card fraud.

Fraud volumes

UK Finance also publishes the number of fraud incidents to convey more fully the dynamics of the fraud environment in the UK. There was a significant rise in the number of cases involving remote purchase fraud and card ID theft in 2018, which has driven the overall rise in fraud volumes. However, the resulting gross losses showed smaller increases, indicating that cases are being spotted and stopped by card issuers more quickly, with a lower average loss per case.

Fraud Type	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	% Change 17/18
Remote Purchase (CNP)	266.4	226.9	221.0	247.3	301.0	331.5	398.4	432.3	408.4	506.4	24%
Of which e-commerce	153.2	135.1	139.6	140.2	190.1	219.1	261.5	310.3	310.4	393.4	27%
Counterfeit	80.9	47.6	36.1	42.3	43.3	47.8	45.7	36.9	24.2	16.3	-33%
Lost & Stolen	47.2	44.2	50.1	55.4	58.9	59.7	74.1	96.3	92.9	95.1	2%
Card ID Theft	38.1	38.1	22.5	32.6	36.7	30.0	38.2	40.0	29.8	47.3	59%
Card not-received	6.9	8.4	11.3	12.8	10.4	10.1	11.7	12.5	10.2	6.3	-38%
TOTAL	**439.5**	**365.2**	**341**	**390.4**	**450.2**	**479.1**	**568.1**	**618.1**	**565.4**	**671.4**	**19%**
UK	316.8	271.4	260.9	288.4	328.2	328.7	379.7	417.9	407.5	496.6	22%
Fraud Abroad	122.6	93.9	80.0	102.0	122.0	150.3	188.4	200.1	158.0	174.8	11%

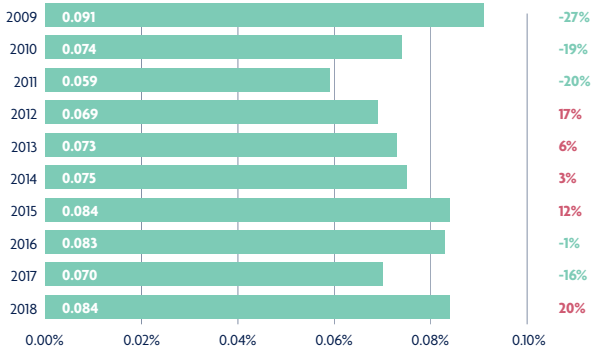
Due to the rounding of figures, the sum of separate items may differ from the totals shown.
E-commerce figures are estimated.

Annual case volumes on UK-issued cards 2013 – 2018

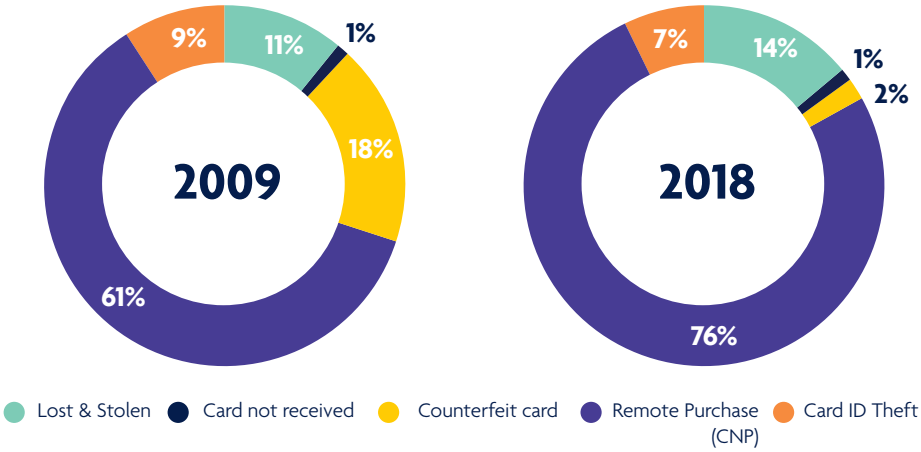
It is important to note that the number of cases relates to the number of accounts that have been defrauded, as opposed to the number of victims.

Card Fraud Type on UK-issued credit and debit cards	2013	2014	2015	2016	2017	2018	% Change 17/18
Remote Purchase (CNP)	951,998	1,019,146	1,113,084	1,437,832	1,398,153	2,050,275	47%
Counterfeit (skimmed/cloned)	101,109	99,279	86,021	108,597	85,025	58,636	-31%
Fraud on lost or stolen cards	138,967	133,943	143,802	231,164	350,279	434,991	24%
Card ID theft	30,718	26,542	33,566	31,756	29,156	63,791	119%
Card not-received	9,125	9,302	10,719	11,377	10,903	10,046	-8%
TOTAL	**1,231,917**	**1,288,212**	**1,387,192**	**1,820,726**	**1,873,516**	**2,617,739**	**40%**

Fraud to turnover ratio 2009 - 2018



Card fraud losses 2018 split by type (as a percentage of total losses)



Remote purchase (Card-not-present) fraud (internet, telephone, mail order)

VALUE	£506.4m	24%

VOLUME	2,050,275	47%

This fraud occurs when a criminal uses stolen card details to buy something on the internet, over the phone or through mail order.

Overall remote purchase fraud increased to £506.4 million in 2018; a rise of 24 per cent when compared to 2017. Online fraud against UK retailers totalled an estimated £265.1 million in 2018, a rise of 29 per cent on the previous year. Mail and telephone order (MOTO) fraud against retailers based in the UK also increased, rising 14 per cent to £92.1 million.

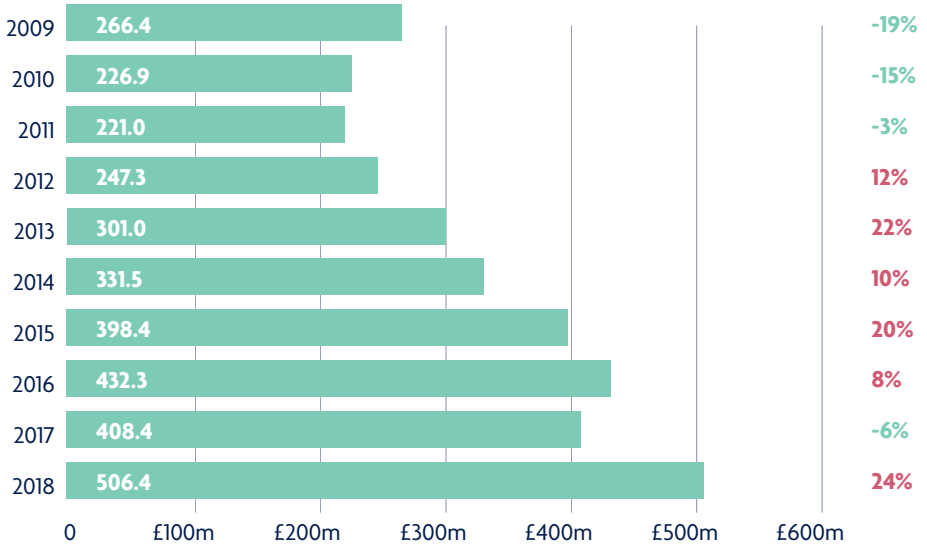
While the number of cases of remote purchase fraud increased by 47 per cent in 2018, the gross loss rose by the lower level of 24 per cent, suggesting that card issuers are identifying and stopping individual incidents more quickly.

During the same period there was a 24 per cent increase in genuine remote purchase transactions, totalling 5.9 billion in 2018, with a 14 per cent increase in value to £387.1 billion. This means that as a proportion of spending, remote purchase fraud is 13p in every £100 spent, up from 12p in 2017.

Intelligence suggests that this type of fraud results mainly from the criminal use of card details that have been obtained through data compromise, including third-party data breaches, phishing emails and scam text messages. There has been a number of high-profile data breaches affecting UK cardholders in 2018, as well as lower-profile attacks, which have driven the increase in remote purchase fraud, with criminals using the stolen data to make unauthorised purchases online, in particular. This is demonstrated by the fact that 78 per cent of all remote purchase fraud took place online (£393.4 million).

Criminals also use social media profiles to advertise the 'sale' of discounted goods to consumers. When a customer goes to buy the product, the criminal uses their card details to purchase the item from a legitimate source and then keeps the payment from the customer.

Remote purchase (CNP) fraud losses on UK-issued cards 2009 - 2018



How to stay 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.
- 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 offer.

Counterfeit Card Fraud

VALUE	£16.3m	-33%

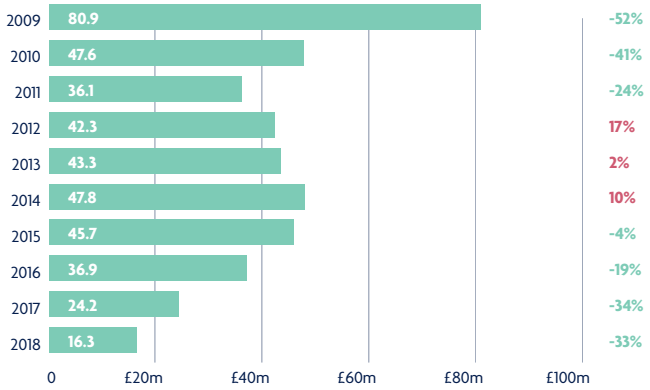
VOLUME	58,636	-31%

This fraud occurs when a criminal creates a fake card using information obtained from the magnetic stripe. Counterfeit card losses totalled £16.3 million in 2018, a decrease of 33 per cent compared to 2017 and 90 per cent lower than the peak reported in 2008 (£169.8 million).

To obtain the data required to create a counterfeit card, criminals commonly attach concealed or disguised devices to the card-reader slots of ATMs and unattended payment terminals (UPTs), such as self-service ticket machines at railway stations, cinemas and car parks. The counterfeit cards are typically used overseas in countries yet to upgrade to Chip and PIN.

The significant decrease in this type of fraud since 2008 is likely to be a result of the introduction of chip technology in the UK and its subsequent increased adoption around the world, most notably in the United States.

Counterfeit card fraud losses on UK-issued cards 2009 – 2018



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.

Lost and Stolen Card Fraud

VALUE	£95.1m	2%

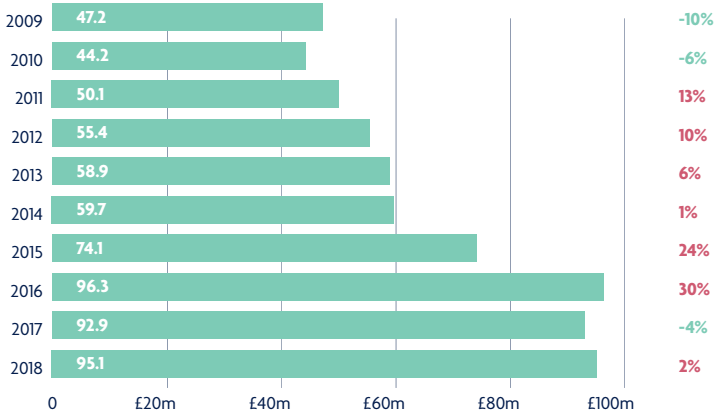
VOLUME	434,991	24%

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 rose by two per cent in 2018 to £95.1 million. The number of incidents increased by 24 per cent during the same period, 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. The frequency of this will vary between card issuers. From September 2019, new rules (the EU's second Payment Services Directive (PSD2)) will require a PIN once a customer's total contactless payments exceed a cumulative value of roughly £130 (€150) or when five contactless payments have been made.

With the rollout of chip technology in the UK and around the world leading to significant decreases in counterfeit card losses, criminals are using more low-tech methods. To carry out this type of fraud criminals use tactics including distraction thefts and card entrapments at ATMs. To obtain the PIN, criminals typically shoulder-surf victims in shops and at ATMs. Criminals also use small cameras, attached to ATMs and directed at the keypad to capture PINs. In some cases, the victims are even tricked into handing their cards and PINs over to a criminal on their own doorstep, under the impression they are assisting with a police enquiry.

Lost and stolen card fraud losses on UK-issued cards 2009 – 2018



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 ID theft

VALUE	£47.3m	59%

VOLUME	63,791	119%

Card ID theft occurs when a criminal uses a fraudulently obtained card or card details, along with stolen personal information, to open or take over a card account held in someone else's name. This type of fraud is split into two categories, third-party application fraud and account takeover fraud.

Losses due to card ID theft rose by 59 per cent in 2018 to £47.3 million, with the number of cases increasing by 119 per cent to 63,791.

Intelligence suggests that the main driver of card ID theft is data harvesting by criminals through methods including phishing emails, scam texts and the theft of mail from external mail boxes and multi-occupancy buildings.

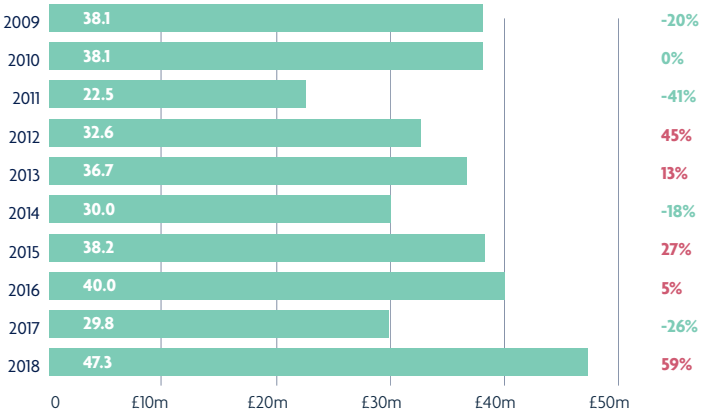
Application fraud – £29.4 million (159%)

Application fraud occurs when criminals use stolen or fake documents to open an account in someone else's name. For identifications purposes, criminals may try to steal documents such as utility bills and bank statements to build up useful personal information. Alternatively, they may use counterfeit documents.

Account takeover - £17.9 million (-3%)

Account takeover involves a criminal fraudulently using another person's credit or debit card account, first by gathering information about the intended victim, then contacting the card issuer pretending to be the genuine cardholder.

Card ID theft fraud losses on UK-issued cards 2009 – 2018



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 bank or building society branch.

Card not-received fraud

VALUE	£6.3m	-38%

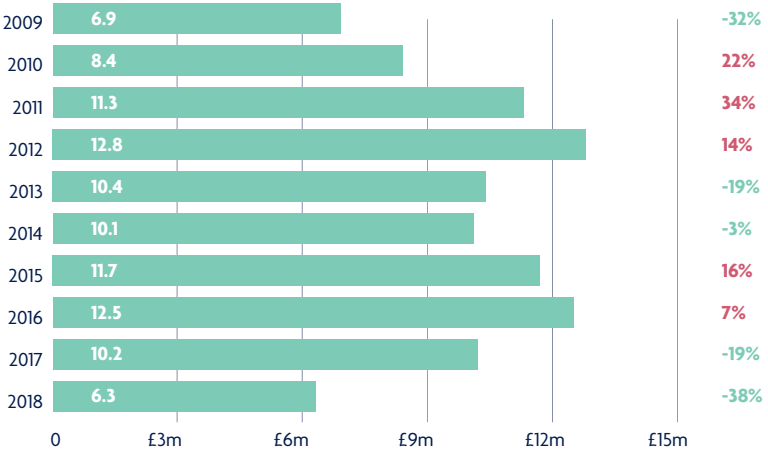
VOLUME	10,046	-8%

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

Card not-received fraud losses fell by 38 per cent in 2018 to £6.3 million.

Criminals typically target properties with communal letterboxes, such as flats and student halls of residence, and external mail boxes to commit this type of fraud. People who do get their mail redirected when they change address are also vulnerable to this type of fraud.

Card not-received fraud losses on UK-issued cards 2009-2018



How to stay safe from card not-received fraud:

- If you are expecting a new card and it hasn't arrived, call your bank or card company for an update.
- Tell your bank or card issuer immediately if you move home. Ask Royal Mail to redirect your post to your new address for at least a year.
- Be extra careful if you live in a property where other people have access to your mail, such as a block of flats. In some cases, your card company may arrange for you to collect your cards from a local branch.

Further card fraud analysis

PLEASE NOTE: Figures in the following sections relate to the places where the card was used fraudulently, rather than how the card or the card details were compromised. This is simply another way of breaking the overall card fraud totals and so these figures should not be treated as an addition to those already covered in the earlier sections. Case volumes are not available for the place of misuse, as it is feasible that one case could cover multiple places, e.g. a lost or stolen card could be used to make an ATM withdrawal as well as to purchase goods on the high street.

UK retail face-to-face card fraud losses

VALUE	£ 69.8m	13%

UK retail face-to-face card 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 13 per cent in 2018 to £69.8 million.

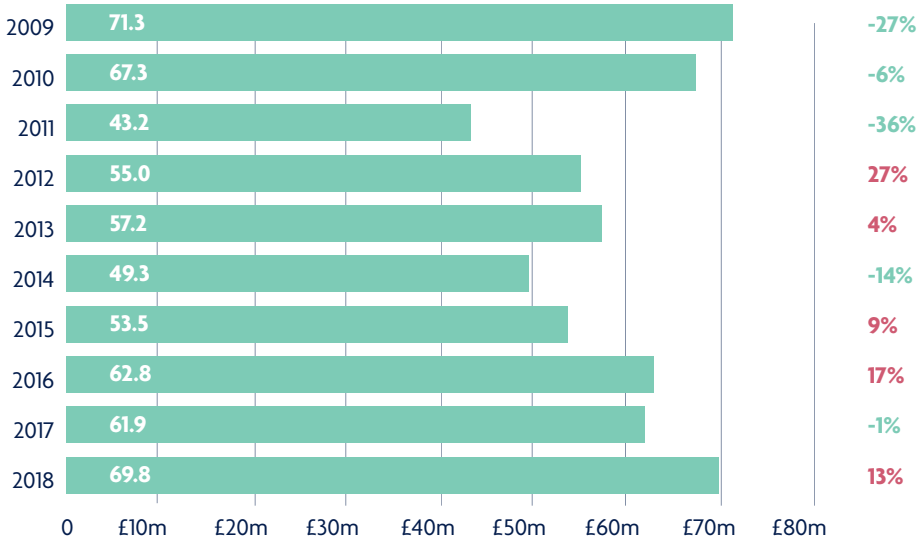
The majority of this fraud is undertaken using low-tech techniques, with fraudsters finding ways of stealing the card, and often the PIN, to carry out fraudulent transactions in shops. This includes criminals using methods such as ATM card entrapment and distraction thefts, combined with shoulder surfing and PIN pad cameras. Criminals also use various social engineering methods to dupe victims into handing over their cards on their own front door step, often known as courier scams.

This category includes fraud incidents involving the contactless functionality on both payment cards and mobile devices. Fraud using the contactless technology on payment cards and devices remains low, with £19.5 million of losses during 2018, compared to spending of £69 billion over the same period.

This is equivalent to 2.7p in every £100 spent using contactless technology, the same level recorded in 2016 and 2017. Fraud using the contactless technology on payment cards and devices represents just 2.9 per cent of overall card fraud losses, while 36 per cent of all card transactions were contactless last year.

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. The frequency of this will vary between card issuers. From September 2019, new rules (the EU's second Payment Services Directive (PSD2)) will require a PIN once a customer's total contactless payments exceed a cumulative value of roughly £130 (€150) or when five payments have been made.

Card Fraud Losses at UK retailers (face-to-face transactions) 2009-2018



Internet/e-commerce card fraud losses

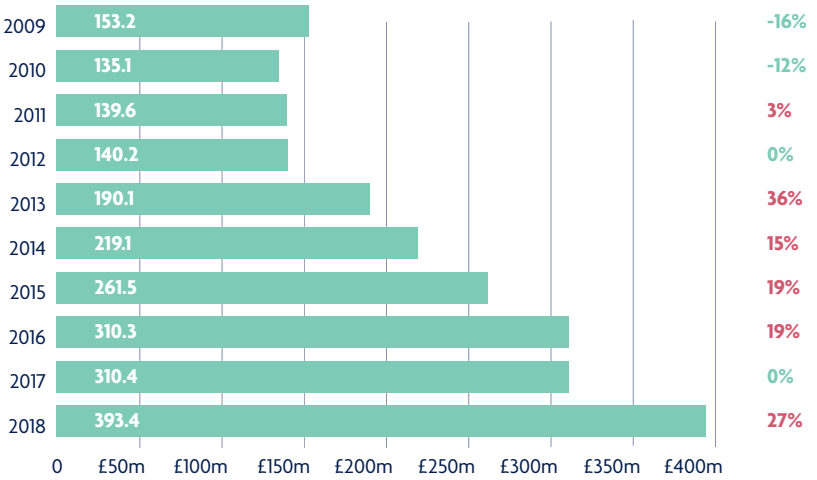
VALUE	£ 393.4m	27%

These figures cover fraud losses on card transactions made online and are included within the overall remote purchase (card-not-present) fraud losses described in the previous section. An estimated £393.4 million of e-commerce fraud took place on cards in 2018, accounting for 59 per cent of all card fraud and 78 per cent of total remote purchase fraud.

Data compromise, including through data hacks at third parties such as retailers, is a major driver of these fraud losses, with criminals using the stolen card details to make purchases online. There were several high-profile data breaches occurring in 2018, with significant brands affected, alongside a number of lower-level incidents. The data stolen from a breach can be used for months or even years after the incident. Criminals also use the publicity around data breaches as an opportunity to trick people into revealing financial information.

Total e-commerce sales on sites based in the UK during 2018 was £251 billion, meaning that for every £100 spent online at UK merchants only 10.5p was fraudulent. For online merchants based overseas, 25p for every £100 was fraudulent.

Internet/e-commerce fraud losses on UK issued cards 2009-2018



Card fraud at UK cash machines

VALUE	£ 32.6m	-12%

These figures cover fraudulent transactions made at cash machines in the UK, either using a stolen card or where a card account has been taken over by the criminal. In all cases the fraudster would need to have access to the genuine PIN and card. Some losses result from cardholders keeping their PIN written down in a purse or wallet, which is then stolen, as well as distraction thefts in shops and bars.

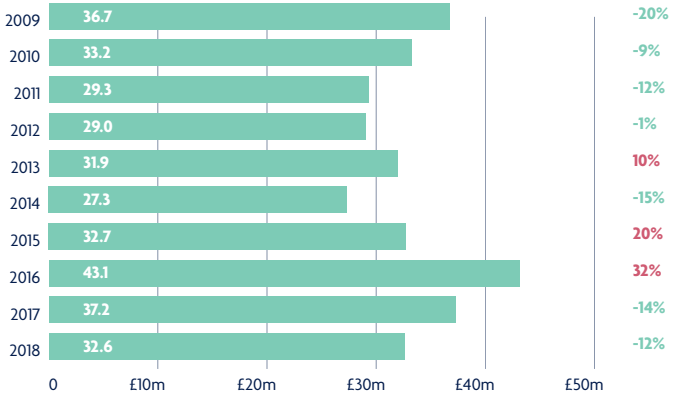
Fraudsters also target cash machines to compromise or steal cards or card details in three main ways:

Entrapment devices: Inserted into the card slot in a cash machine, these devices prevent the card from being returned to the cardholder. To capture the PIN, the criminal will use a small camera attached to the machine and directed at the PIN pad, or they will watch it being entered by the cardholder. Once the customer leaves the machine, the criminal removes the device and the card and subsequently uses it to withdraw cash.

Skimming devices: These devices are attached to the cash machine to record the details from the magnetic strip of a card, while a miniature camera captures the PIN being entered. A fake magnetic stripe card is then produced and used with the genuine PIN to withdraw cash at machines overseas which have yet to be upgraded to Chip & PIN.

Shoulder surfing: A technique used by criminals to obtain PINs by watching over the cardholder's shoulder when they are using an ATM or card machine. The criminal then steals the card using distraction techniques or pickpocketing.

Fraud losses at UK cash machines 2009-2018



Card fraud abroad

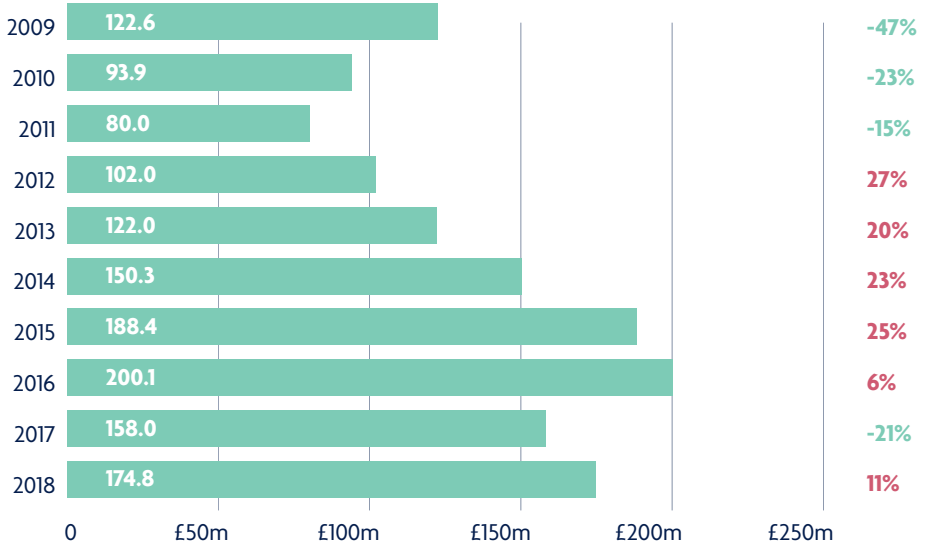
VALUE	£ 174.8m	11%

This category covers fraud occurring in locations overseas on UK-issued cards. The majority (85 per cent) of this type of fraud is attributed to remote purchase fraud at overseas retailers.

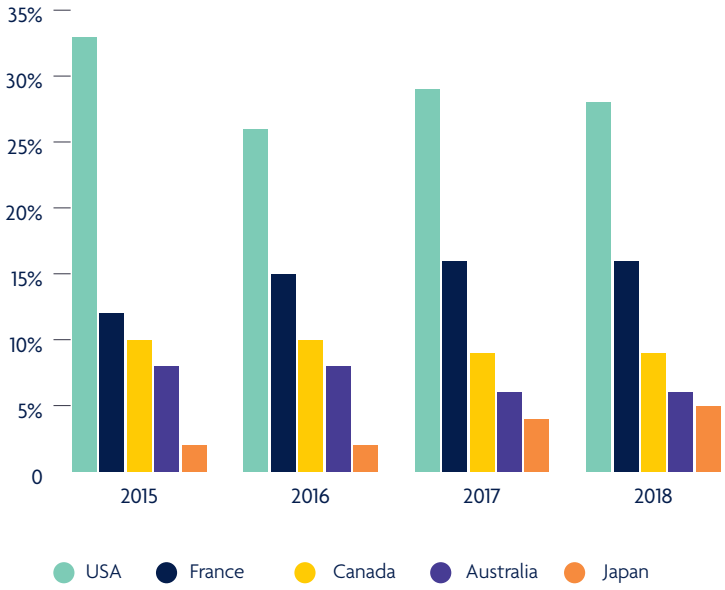
This category also includes cases where criminals steal the magnetic stripe details from UK-issued cards to make counterfeit cards, which are then used overseas in countries yet to upgrade to Chip & PIN.

International fraud losses for 2018 were £174.8 million, compared with losses at their peak in 2008 of £230.1 million, a decrease of 24 per cent.

Fraud committed abroad on UK-issued cards 2009-2018

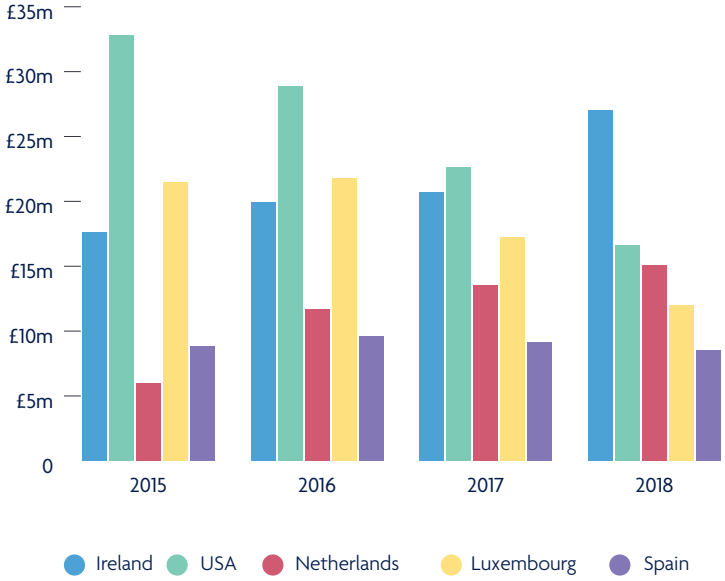


Top five countries for fraud on Foreign-issued cards occuring in the UK 2015-2018



Top five countries where fraud on UK-issued cards occurs 2015-2018

Losses on UK-issued cards or card details used fraudulently overseas.



CHEQUE FRAUD

Cheque Fraud

VALUE	£20.6m	109%

VOLUME	2,020	16%

Cheque fraud losses increased to £20.6 million in 2018. This is the first rise in cheque fraud reported in seven years. The volume of fraudulent cheques increased by only 16 per cent, indicating that a small number of high-value fraudulent transactions led to the rise in losses last year, rather than any change to the longer-term trend.

A total of £218.2 million of cheque fraud was prevented in 2018, up by three per cent on 2017. This is equivalent to £9.14 in every £10 of attempted cheque fraud being stopped before a loss occurs. This remains the highest proportion of attempted fraud prevented across all types of fraud.

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

Counterfeit cheque fraud - £15.9 million +486%

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

Forged cheque fraud - £3.4 million -20%

A forged cheque is a genuine cheque that has been stolen from a customer and used by a fraudster with a forged signature.

Fraudulently altered cheques - £1.2 million -56%

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

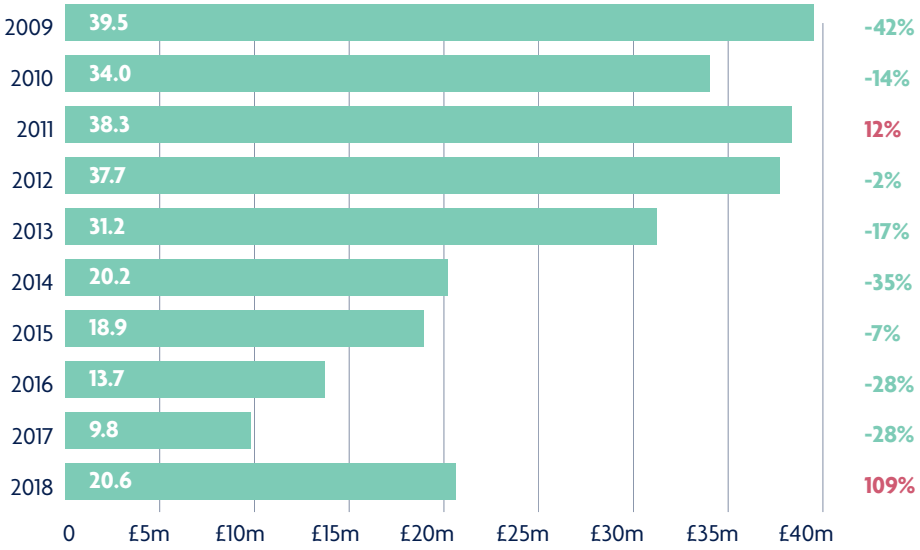
Prevented Cheque Fraud 2015 - 2018

Year	2015	2016	2017	2018	% change 17/18
Cheque Fraud	£392.8m	£196.2m	£212.3m	£218.2m	3%

Annual case volumes cheque fraud 2014-2018

Year	2014	2015	2016	2017	2018	% change 17/18
Cheque Fraud	8,168	5,746	3,388	1,745	2,020	16%

Cheque Fraud losses 2009-2018



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

UNAUTHORISED REMOTE BANKING FRAUD

Unauthorised remote banking fraud

VALUE	£152.9m	-2%

VOLUME	31,797	-8%

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.

Total remote banking fraud totalled £152.9 million in 2018, two per cent lower than compared to 2017. The number of cases of remote banking fraud fell by eight per cent to 31,797.

A total of £317.7 million of attempted remote banking fraud was stopped by bank security systems during 2018. This is equivalent to £6.75 in every £10 of fraud attempted being prevented. In addition, 15 per cent (£22.2 million) of the losses across all remote banking channels was 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.

Remote Banking values	2012	2013	2014	2015	2016	2017	2018	17/18 % Change
Internet Banking	£57.0m	£58.8m	£81.4m	£133.5m	£101.8m	£121.2m	£123.0m	1%
Telephone Banking	£14.7m	£13.1m	£16.8m	£32.3m	£29.6m	£28.4m	£22.0m	-22%
Mobile Banking	N/A	N/A	N/A	£2.8m	£5.7m	£6.5m	£7.9m	20%
TOTAL	**£71.7m**	**£71.9m**	**£98.2m**	**£168.6m**	**£137.0m**	**£156.1m**	**£152.9m**	**-2%**

Remote Banking cases	2012	2013	2014	2015	2016	2017	2018	17/18 % Change
Internet Banking	16,355	13,799	16,041	19,691	20,088	21,745	20,904	-4%
Telephone Banking	7,095	5,596	5,778	11,380	10,495	9,577	7,937	-17%
Mobile Banking	N/A	N/A	N/A	2,235	2,809	3,424	2,956	-14%
Total	**23,450**	**19,395**	**21,819**	**33,306**	**33,392**	**34,746**	**31,797**	**-8%**

Internet banking fraud

VALUE	£123.0m	1%

VOLUME	20,904	-4%

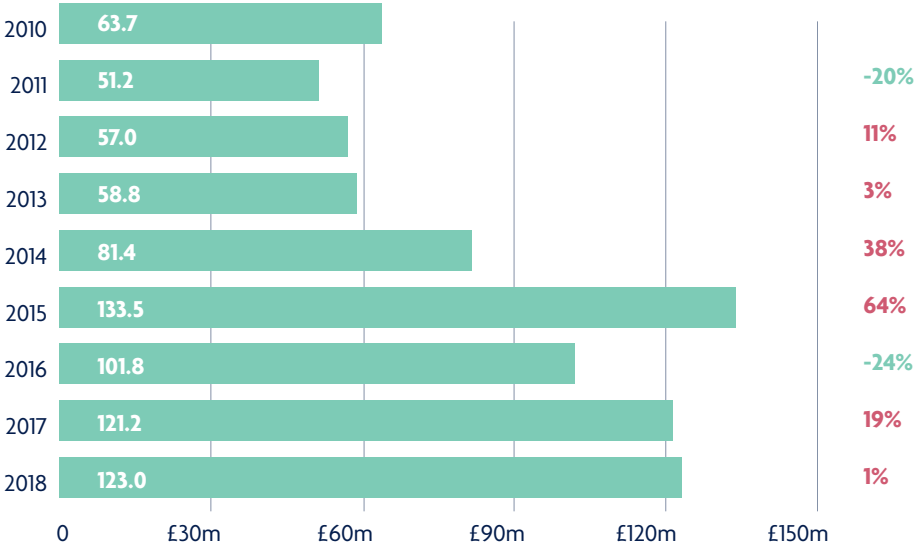
This type of fraud occurs when a fraudster gains access to a customer's online bank account and makes an unauthorised transfer of money.

This form of fraud is facilitated by criminals' use of social engineering tactics to trick customers into revealing their online banking security details. These include impersonation scams using phone calls, texts and emails which often claim there has been suspicious activity on a bank or card 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.

In addition, 15 per cent (£18.8 million) of the losses across the internet banking channel was recovered after the incident.

Collection of industry fraud losses for internet banking began in June 2009.
Case volumes were not collected until 2012.

Internet banking fraud losses 2010-2018



Annual case volumes for internet banking fraud 2012-2018

	2012	2013	2014	2015	2016	2017	2018	17/18 % Change
Internet Banking fraud	16,355	13,799	16,041	19,691	20,088	21,745	20,904	-4%

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

VALUE	£22.0m	-22%

VOLUME	7,937	-17%

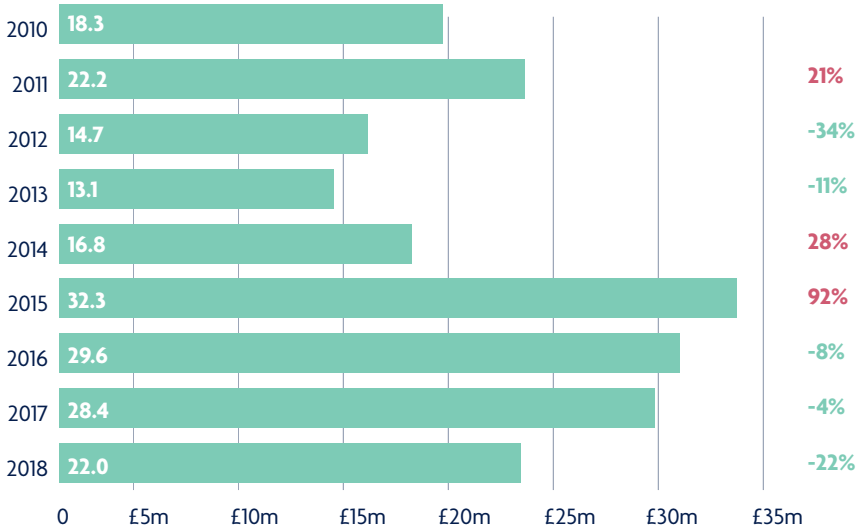
This type of fraud occurs when a criminal gains access to the victim's telephone banking account and makes an unauthorised transfer of money from it.

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

In addition, nine per cent (£1.9 million) of the losses across the telephone banking channel was recovered after the incident.

Collection of industry fraud losses for telephone banking fraud began in June 2009. Case volumes were not collected until 2012.

Telephone banking fraud losses 2010-2018



Annual case volumes for telephone banking fraud 2012-2018

	2012	2013	2014	2015	2016	2017	2018	17/18 % Change
Telephone Banking fraud	7,095	5,596	5,778	11,380	10,495	9,577	7,937	-17%

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

VALUE	£7.9m	20%

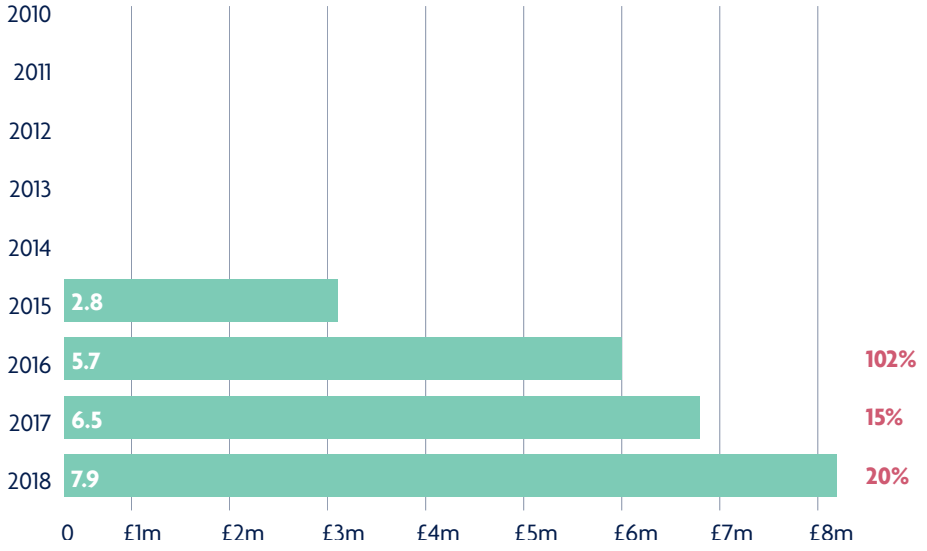
VOLUME	2,956	-14%

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

Rises are to be expected in the mobile banking channel as the level of usage increases amongst customers. 48 per cent of adults living in the UK now use a mobile banking app, either on their telephone or tablet, up from 33 per cent in 2015.

In addition, 18 per cent (£1.4 million) of the losses across the mobile banking channel was recovered after the incident.

Mobile banking fraud losses 2015-2018



Annual case volumes for mobile banking fraud 2012-2018

	2012	2013	2014	2015	2016	2017	2018	17/18 % Change
Mobile banking fraud	N/A	N/A	N/A	2,235	2,809	3,424	2,956	-14%

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

AUTHORISED PUSH PAYMENT (APP) FRAUD

Authorised Push Payment (APP) Fraud

VALUE	£354.3m	50%

VOLUME	84,624	93%

UK Finance began collating and publishing data on authorised push payment 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 now includes the scam type, payment type and payment channel.

While the data for 2017 is included in the overall figures below, 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.

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.

Losses due to authorised push payment scams were £354.3 million in 2018. This was split between personal (£228.4 million) and non-personal or business (£126 million).

In total there were 84,624 cases relating to a total of 83,864 victims. Of this total, 78,215 cases were on personal accounts and 6,409 cases were on non-personal accounts.

Criminals' use of social engineering tactics through deception and impersonation scams is a key driver of authorised push payment scams. Typically, this involves 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. Criminals also use social media to approach victims, using adverts for goods and investments which never materialise once the payment has been made.

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. This can make it difficult for banks to trace the stolen money, however the industry has been working with Pay.UK to implement new technology that will help track suspicious payments and identify money mule accounts.

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

In February 2019, following work between the industry, consumer groups and the regulator, a new authorised push payment (APP) scams Voluntary Code was published. The Code will bring new protections for customers of signatory payment service providers and will be implemented on 28 May 2019. The Code delivers a significant commitment from all firms who sign up to it to reimburse victims of authorised push payment scams in any scenario where their bank or payment service provider is at fault and the customer has met the standards expected of them under the Code.

		PERSONAL			NON PERSONAL			TOTAL		
		2017	2018	% Change	2017	2018	% Change	2017	2018	% Change
Volume	Cases	38,596	78,215	103%	5,279	6,409	21%	43,875	84,624	93%
	Payments	N/A	114,707	N/A	N/A	8,950	N/A	N/A	123,657	N/A
Value	Value	£107.5m	£228.4m	112%	£128.6m	£126m	-2%	£236.0m	£354.3m	50%
	Repatriation	£22.6m	£42.3m	87%	£38.2m	£40.3m	5%	£60.8m	£82.6m	38%

DEFINITIONS:

- **Cases:** The total volume of confirmed APP fraud cases identified during the reporting period.
- **Payments:** The total number of fraudulent payments associated with the total APP fraud cases.
- **Value:** The total value of confirmed APP fraud cases identified during the reporting period.
- **Repatriation:** Combination of refunds (cases where the victim has received either a full or partial refund directly from their bank) and recoveries (cases where funds have been recovered from the recipient bank).

The finance industry is tackling authorised push payment scams by:

- Working with consumer groups to develop a Voluntary Code to better protect customers and reduce the occurrence of APP fraud. The Code was published in February and will become effective for signatory firms on 28 May 2019.
- Helping to prevent customers being duped by criminals by raising awareness of scams and how to stay safe through the Take Five to stop Fraud campaign in conjunction with the Home Office.
- 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 2018 it prevented £38 million in fraud and led to 231 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 2018 the Unit prevented an estimated £94.5 million of fraud, secured 48 convictions and disrupted 11 organised crime groups.

- Working with Pay.UK to implement Mule Insights Tactical Solution (MITS), a new technology that will help track suspicious payments and identify money mule accounts.
- Implementing standards to ensure those who have fallen victim to fraud or scams get the help they need.
- Working with Pay.UK to implement Confirmation of Payee, an account name checking service for when a payment is being made that will help to prevent authorised push payment scams.
- 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, so that it meets the needs of crime agencies, regulators, consumers and businesses.
- Working closely with mobile network operators and the messaging industry to trial a new anti-spoofing system to help root out scam text messages.

Further analysis of the APP scam data

Since 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).
- **Five payment types:** Faster Payments, CHAPS, Bacs, 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 in the previous section and is not in addition to the total figures.

As the data was collated for the first time in 2018, comparisons with the previous year are not available.

SCAM TYPES

Malicious Payee

Purchase Scam

VALUE £46.4m **VOLUME 52,621**

In a purchase scam, the victim pays in advance for goods or services that are never received. These scams usually involve the victim using an online platform such as an auction website or social media.

Common scams include a criminal posing as the seller of a car or a technology product, such as a phone or computer, which they advertise at a low price to attract buyers. Criminals also advertise items such as 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. When the victim transfers the money, the seller disappears, and no goods or services arrive.

Purchase scams were the most common form of APP scam in 2018, with the 52,621 cases accounting for 62 per cent of the total number of APP scam cases. A total of £46.4 million was lost to purchase scams in 2018, with the vast majority of losses being from personal accounts. Payment service providers were subsequently able to return £4.3 million of the losses.

Typically purchase scams involve lower-value payments, with the smaller average case value meaning that they accounted for only 13 per cent of the total value of APP scams.

Purchase scams 2018	Personal	Non Personal	Total
Number of cases	51,208	1,413	52,621
Number of payments	65,033	1,663	66,696
Value of losses	£42.4m	£4.0m	£46.4m
Returned to customer	£3.8m	£0.5m	£4.2m

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

VALUE £50.1m **VOLUME 3,385**

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 will usual promise a high return in order to entice their victim into making the transfer. These scams include investments in items such as gold, property, carbon credits, cryptocurrencies, land banks and wine.

The criminals behind investment scams often use cold calling to target their victim and pressurise them to act quickly by claiming the opportunity is time-limited. Email, social media and letters are also used in investment scams, with criminals seeking to take advantage of recent pension reforms.

A total of £50.1 million was lost to investment scams in 2018, with payment services providers subsequently able to return £3.9 million. The nature of the scams means that the sums involved in individual cases can be higher, so while investment scams accounted for only four per cent of the total number of APP scam cases, they accounted for 14 per cent of the total value.

Investment scams 2018	Personal	Non Personal	Total
Number of cases	3,312	73	3,385
Number of payments	7,795	141	7,936
Value of losses	£48.5m	£1.6m	£50.1m
Returned to customer	£3.7m	£0.2m	£3.9m

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 and follow the advice of its ScamSmart campaign.
- 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

VALUE £12.6m **VOLUME 1,404**

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. Fraudsters will use fake profiles to target their victims in an attempt to start a relationship which they will try to develop over a long period of time. Once they have established their victim's trust, the criminal will then claim to be experiencing a problem, such as an issue with a visa, health issues or flight tickets and ask for money to help.

A total of £12.6 million was lost to romance scams in 2018. The nature of the scam means that the individual is often convinced to make multiple, generally smaller, payments to the criminal, as indicated by an average of around five payments per case. Romance scams accounted for two per cent of the total number of APP scam cases in 2018 and four per cent of the total value. Payment service providers were only able to return £640,000 of the losses, often due to the fact that the payments were made over an extended period meaning the criminal had moved the money by the time the scam was reported.

Romance scams 2018	Personal	Non Personal	Total
Number of cases	1,400	4	1,404
Number of payments	7,557	17	7,574
Value of losses	£12.5m	£0.1m	£12.6m
Returned to customer	£0.6m	£0.0m	£0.6m

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

VALUE £14.0m **VOLUME 8,133**

In an advance fee scam, a criminal convinces their victim to pay a fee which they claim would result in the release of a much larger payment or high-value goods. These scams include claims from the criminals that the victim has won an overseas lottery, that gold or jewellery is being held at customs or that an inheritance is due. The fraudster tells the victims that a fee must be paid to release the funds or goods, however, when the payment is made, the promised goods or money never materialises. These scams often begin with an email or a letter sent by the criminal to the victim.

Advance fee scams were the second most common form of APP scam in 2018, accounting for ten per cent of the total number of cases. A total of £14 million was lost to advance fee scams last year, meaning by value these scams accounted for four per cent of all APP scams.

Advance fee scams 2018	Personal	Non Personal	Total
Number of cases	7,915	218	8,133
Number of payments	12,876	395	13,271
Value of losses	£12.8m	£1.2m	£14m
Returned to customer	£1.1m	£0.3m	£1.4m

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.

Malicious Redirection

Invoice and mandate scams

VALUE	£123.7m	VOLUME	7,544

In an invoice or mandate scam, the victim attempts to pay an invoice to a legitimate payee, but the criminal intervenes to convince the victim to redirect the payment to an account they control. 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. This type of fraud often involves the criminal either intercepting emails or compromising an email account.

Invoice and mandate scams were the third most common type of APP scam in 2018, however they resulted in the largest share of losses at 35 per cent, totalling £123.7 million. The majority of losses by value, some £92.7 million, were from non-personal or business accounts, where the average payment was £20,750. This reflects the fact that businesses make higher-value payments more regularly.

Invoice and mandate scams 2018	Personal	Non Personal	Total
Number of cases	4,274	3,280	7,544
Number of payments	5,431	4,467	9,898
Value of losses	£31.0m	£92.7m	£123.7m
Returned to customer	£6.8m	£29.6m	£36.4m

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

VALUE	£14.8m	VOLUME	603

CEO fraud is where the criminal manages to impersonate the CEO of the victim's organisation to convince the victim to make an urgent payment to the scammer's account. This type of fraud mostly affects businesses.

To commit the fraud, 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. The message commonly requests a change to payment details or for a payment to be made urgently to a new account.

CEO fraud was the least common form of APP scam in 2018, accounting for less than one per cent of total cases. A total of £14.8 million was lost, equivalent to four per cent of the total case value.

CEO Fraud 2018	Personal	Non Personal	Total
Number of cases	84	519	603
Number of payments	99	732	831
Value of losses	£1.0m	£13.8m	£14.8m
Returned to customer	£0.2m	£4.2m	£4.3m

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

VALUE £56.5m **VOLUME 5,459**

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 to an account they control.

These scams often begin with a phone call or text message, with the fraudster claiming 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.

To commit this fraud the criminal will often research their victim first, including using information gathered from other scams and data breaches in order to make their approach sound genuine.

Police and bank staff impersonation scams accounted for six per cent of all APP scam cases in 2018. £56.5 million was lost due to these scams, which by value was the second highest type of APP scam, accounting for 16 per cent of total losses. Payment service providers were able to return £19.8 million of the losses to customers.

Impersonation: Police / Bank Staff 2018	Personal	Non Personal	Total
Number of cases	5,112	347	5,459
Number of payments	7,996	707	8,703
Value of losses	£49.8m	£6.7m	£56.5m
Returned to customer	£16.8m	£3.0m	£19.8m

How to stay safe from police/bank 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

VALUE	£36.2m	VOLUME	5,465

In this scam, a criminal claims to represent an organisation such as a utility company, communications service provider or government department. Common scams include claims that the victim must settle a fictitious fine, pay overdue tax or return an erroneous refund. Sometimes the criminal requests remote access to the victim's computer as part of the scam, claiming that they need to help 'fix' a problem.

As with police and bank staff impersonation scams, criminals will often research their targets first, using information gathered from scams, social media and data breaches.

A total of £36.2 million was lost to this type of scam in 2018, with payment service providers subsequently able to return £11.9 million. Impersonation: other scams accounted for six per cent of all APP scam cases last year, representing ten per cent of total losses.

Impersonation: Other 2018	Personal	Non Personal	Total
Number of cases	4,910	555	5,465
Number of payments	7,920	828	8,748
Value of losses	£30.3m	£6.0m	£36.2m
Returned to customer	£9.4m	£2.5m	£11.9m

How to stay safe from other 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

This data shows the type of payment method the victim used to make the payment in the authorised push payment scam.

Faster Payments was used in 93 per cent of payments. While CHAPS was the least common payment method, representing only 0.5 per cent of payments, the high-value nature of transactions using this payment type meant that it made up seven per cent of the total value.

Payment Type	2018	
	Payments	Value
Faster Payments	115,332	£251.6m
CHAPS	652	£26.0m
Bacs	1,454	£23.6m
Intra Bank Transfer ("on us")	1,722	£3.3m
International	4,497	£49.9m
TOTAL	**123,657**	**£354.3m**

PAYMENT CHANNEL

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

Internet banking was used in 76 per cent of payments, totalling £288.7 million of losses.

Payment Channel	2018	
	Payments	Value
Branch	7,919	£41.3m
Internet Banking	93,466	£288.7m
Telephone Banking	4,521	£14.8m
Mobile Banking	17,751	£9.5m
TOTAL	**123,657**	**£354.3m**

TAKE FIVE TO STOP FRAUD

Take Five to Stop Fraud is a national campaign that offers advice to help everyone protect themselves from preventable financial fraud. It is led by UK Finance and backed by the government.

Take Five helps customers to confidently challenge any requests for their personal or financial information, or to transfer money to a fraudster's account. It focuses on financial frauds directly targeting customers, including email deception and phone-based scams as well as online fraud – particularly where criminals impersonate trusted organisations.

The campaign is being delivered with and through a range of partners in the UK payments industry, financial services firms, law enforcement agencies, telecommunication providers, commercial, public and third sector organisations.

To help everyone stay safe from fraud and scams, Take Five to Stop Fraud urges customers to follow the campaign advice:

- 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.

To find out more about Take Five visit www.takefive-stopfraud.org.uk

TAKE FIVE TO STOP FRAUD™