UK FINANCE

FRAUD - THE FACTS 2020

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 cyber-enabled crime.

UK Finance seeks to ensure that the UK is the safest and most transparent financial centre in the world - thus creating a hostile environment for criminals by working with members, law enforcement, government agencies and industry. 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 our Economic Crime Industry Intelligence Unit 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 and Don't Be Fooled) to inform customers about threats and how to stay safe. This includes the Take Five Charter.
- Informing commentators and policymakers through our press office and public affairs functions.
- Implementing procedures between police and bank branches to prevent vulnerable people falling victim to fraud (Banking Protocol),
- Assessing the impact of new technologies, 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 continues to pose a major threat to the UK and as criminals become ever more imaginative in their attempts to steal customers' money, this shows no sign of changing.

Our Fraud – the Facts 2020 report highlights that last year investment by the finance industry in advanced security systems to protect customers prevented more than £1.8 billion of unauthorised fraud. But criminals still successfully stole over £1.2 billion through fraud and scams in 2019.

Despite the many steps taken by the finance industry the battle continues and new fronts have opened up in recent years, in particular the huge growth in fraud being driven by online adverts and social media content. These include romance scams perpetrated by fraudsters on online dating sites; investment fraud – where criminals often advertise seemingly authentic investment opportunities online but in fact the whole project is a scam; and purchase fraud where goods are advertised online and on auction sites at 'too good to be true' rates in order to entice people to buy, but again, in most cases it is likely to be a scam. Fraudsters have also increasingly been targeting younger people online through 'Money Mule' adverts offering students and young people in particular money to have funds transferred through their bank account and back out again, which is effectively money laundering.

The DCPCU (the specialist police unit funded by the banking and finance industry that targets the organised criminal gangs responsible for fraud) has used new partnerships with social media platforms to identify and take down accounts with posts related to payment crime. In total over 1,600 social media accounts linked to fraudulent activity have been taken down. Of these, almost 500 were used to recruit young people as money mules, while nearly 250 were involved in the trading of stolen card details online.

As an industry we have been working with the government on a national economic crime plan. The publication of this in July 2019 laid out the intended strategy to tackle economic crime for the next three years and was warmly welcomed. However, UK Finance is now calling on the government to include economic crime in the forthcoming regulatory framework on online harms to ensure greater protection for the many customers who become victims of economic crime. Incorporating economic crime within this regulatory framework will help to harness the capabilities, expertise and powers of both the public and private sectors to truly create a step change in approach. It will also ensure online service providers play their part in tackling harms such as fraud and scams which fund further criminality.

Breaches at third parties continue to be a major contributor to fraud losses, with several high-profile incidents in 2019 involving well-known brands where customer data was stolen. Whether at a retailer, a utility company, a transport provider or elsewhere, the theft of personal and financial data can

both directly lead to fraud losses and be used by criminals as part of their scams. The data can be used for months – even years – after the breach takes place. These incidents occur outside banks' control, yet it is they and their customers who bear the impact. It is therefore imperative that any organisation that controls customer data does everything in its power to keep them secure.

In the meantime, there are simple steps that can be taken to help protect customers falling prey to unscrupulous fraudsters. For example, encouraging online platforms to carry warnings, share data on known fraudsters and take down their profiles in order to prevent romance fraud scams.

Solicitors and other professionals involved with transfers of customers' money must ensure their own systems are not vulnerable to being hacked and warn customers that last-minute changes to payment accounts are likely to mean fraud is being attempted.

Authorised Push Payment (APP) fraud is a growing problem as criminals increasingly use social engineering tactics to bypass bank security measures and convince customers to transfer funds. APP fraud rose by 29 per cent in value in 2019 compared to the previous year with reported cases up 45 per cent over the same period.

In May 2019 the APP scams voluntary Code was launched to help compensate innocent victims of this form of fraud when they have met the standards expected of them under the Code.

The existence of the Code and the ability to receive compensation is thought to have raised awareness among consumers and driven up the number of people reporting APP scams. Since the introduction of the Code, the amount of money being reimbursed to victims has significantly increased.

However, a voluntary agreement alone is not enough and we strongly believe that issues of liability and reimbursement would best be addressed by new legislation. As is all too clear, these crimes can have a devastating impact on victims. And even if the customer gets the money back, the organised criminal gangs which perpetrate these frauds still profit from the proceeds. Money that is used to fund illicit acts which damage our society – crimes such as terrorism, drug trafficking and people smuggling.

The finance industry is committed to tackling all forms of fraud and protecting people against financial crime, but only the combined efforts of every sector, both public and private, will overcome this blight and ensure that greater protection is available for customers.

KATY WOROBEC
Managing Director: Economic Crime,
UK Finance.

TRENDS AND STATISTICS

2019 overview

Unauthorised financial fraud losses across payment cards, remote banking and cheques totalled £824.8 million in 2019, a decrease of two per cent compared to 2018.

Banks and card companies prevented £1.8 billion in unauthorised fraud in 2019. This represents incidents that were detected and prevented by firms and is equivalent to £6.88 in every £10 of attempted fraud being stopped.

In addition to this, in 2019 UK Finance members reported 122,437 incidents of Authorised Push Payment (APP) scams with gross losses of £455.8 million.

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 increased use by customers and businesses of online services for many different aspects of day to day life is leading criminals to increasingly focus their efforts on defrauding people through online fraud and scams.

For example, in 2019 there was an increase in investment scams as criminals turned to online platforms to try to defraud victims of large sums of money. Previously criminals have typically used cold calling to target victims through investment and pension scams. However, criminals have increasingly moved online and the nature of the frauds has become ever more sophisticated.

Purchase scams have also become increasingly familiar (accounting for 60 per cent of all Authorised Push Payment (APP) volume), as criminals abuse online platforms such as an auction website or social media to target their victims.

Social engineering – a tactic by which criminals groom and manipulate people into transferring money or divulging their personal and financial details – is also commonly used in deception scams. 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.

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 moving money into the criminal's account. These include criminals impersonating a member of bank staff or a police officer, 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; and online auction and sales scams. Fraudsters use a range of methods to contact customers, including by phone, text message, email and social media.

Last year also saw significant increases in cheque fraud as criminals looked to target large corporates, due to the more substantial sums available compared to with personal cheques. This highlights the potential need for security features on corporate cheques to be enhanced to deter fraudsters.

Once again, the theft of personal and financial data through data breaches was a major contributor to fraud losses in 2019. The stolen data is used both to commit fraud 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 customers, using information gained about an individual to add apparent authenticity to a scam.

A number of significant data breaches in 2019 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 the data breach. They cover a range of sectors and occur outside of the control of the banking industry.

UK Finance's Economic Crime Intelligence Unit (I&I) 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. In 2019, there was an 660 per cent increase in the number of card details being repatriated by the unit compared to 2018.

The increase has been caused by the National Cyber Security Centre now using the I&I unit as the mechanism for sharing compromised data found online. 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. Information stolen through a data breach can be used for months or even years after the event.

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.

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 new technology, for example 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 £49.1 million in fraud and enabled 253 arrests in 2019.
- Sponsoring a specialist police unit, the Dedicated Card and Payment Crime Unit (DCPCU), which tackles the organised criminal groups responsible for financial fraud and scams. In 2019, the Unit prevented an estimated £31.2 million of fraud, secured 75 convictions and disrupted 23 organised crime groups.
- The introduction in May 2019 of a voluntary code to help protect customers against APP fraud and reduce the number of cases, as well as treat customers more consistently. A fund set up by the banks that are signatories to the code means customers who fall victim to APP fraud despite having taken precautions will be reimbursed. The fund is in place until the end of this year. However, customers may also be refunded in other ways including by banks that have not signed up to the code.
- Working with Pay.UK to implement the Mule Insights Tactical Solution (MITS), a new technology that helps to track suspicious payments and identify money mule accounts.
- The implementation, with Pay.UK, of Confirmation of Payee (CoP), 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.
- Helping customers stay safe from fraud and spot the signs of a scam through the Take Five and Don't Be Fooled campaigns.
- Working collaboratively with other sectors including the telecoms industry, to address vulnerabilities in the ecosystem.

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.

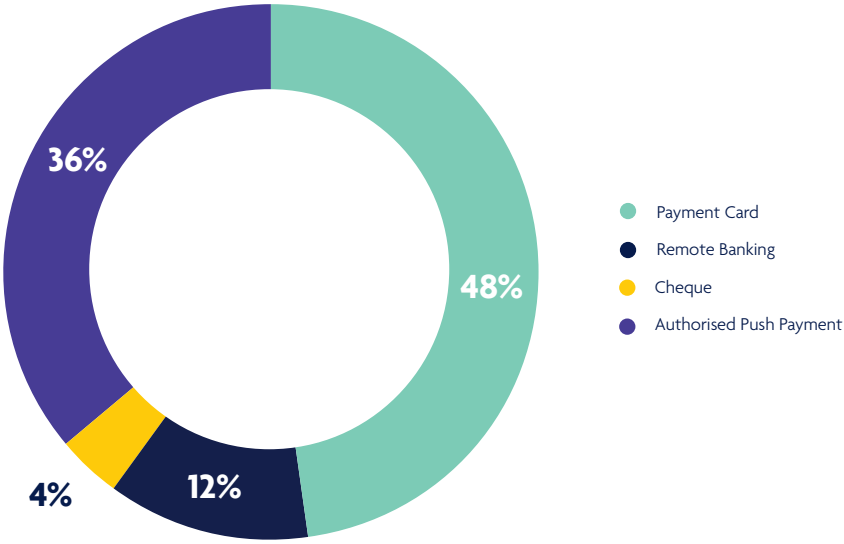
September 2019 saw the start of the phased roll out of new rules requiring all payment providers to use multi-factor authentication for higher-value and higher-risk transactions. The rules mean that when a customer makes certain transactions online, a second level of security would be required, such as a one-time passcode sent via text message or biometrics. The implementation of SCA will take place over 18 months, ending in March 2021.

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.

Total 2019 financial fraud losses by type



CARD FRAUD

Unauthorised debit, credit and other payment card fraud

VALUE	£620.6m	-8%

VOLUME	2,745,539	+5%

Fraud losses on UK-issued cards totalled £620.6 million in 2019, an eight per cent decrease from £671.4 million in 2018. At the same time, total spending on all debit and credit cards reached £829 billion in 2019, with 22 billion transactions made during the year.

Overall card fraud losses as a proportion of the amount we spend on our cards decreased during 2019, falling from 8.4p per £100 spent in 2018 to 7.5p per £100 in 2019 (in 2008 it was 12.4p for every £100 spent).

A total of £999.2 million in card fraud was stopped by banks and card companies in 2019, a decrease of 11 per cent on 2018. This is equivalent to £6.17 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 began to be phased in gradually from September 2019, adding an extra layer of security in the fight against fraud. The roll out will be completed by March 2021.
- 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 Type	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	% Change 18/19
Remote Purchase (CNP)	226.9	221	247.3	301	331.5	398.4	432.3	408.4	506.4	470.2	-7%
Of which e-commerce	135.1	139.6	140.2	190.1	219.1	261.5	310.3	310.4	394.2	359.3	-9%
Counterfeit	47.6	36.1	42.3	43.3	47.8	45.7	36.9	24.2	16.3	12.8	-21%
Lost & Stolen	44.2	50.1	55.4	58.9	59.7	74.1	96.3	92.9	95.1	94.8	0%
Card ID Theft	38.1	22.5	32.6	36.7	30.0	38.2	40.0	29.8	47.3	37.7	-20%
Card non-receipt	8.4	11.3	12.8	10.4	10.1	11.7	12.5	10.2	6.3	5.2	-17%
Total	**365.2**	**341**	**390.4**	**450.2**	**479**	**568.1**	**618.1**	**565.4**	**671.4**	**620.6**	**-8%**
UK	271.4	260.9	288.4	328.2	328.7	379.7	417.9	407.5	496.6	449.9	-9%
Fraud Abroad	93.9	80.0	102.0	122.0	150.3	188.4	200.1	158.0	174.8	170.7	-2%

Due to the rounding of figures, the sum of separate items may differ from the totals shown.

E-commerce figures are estimated.

Card fraud volumes

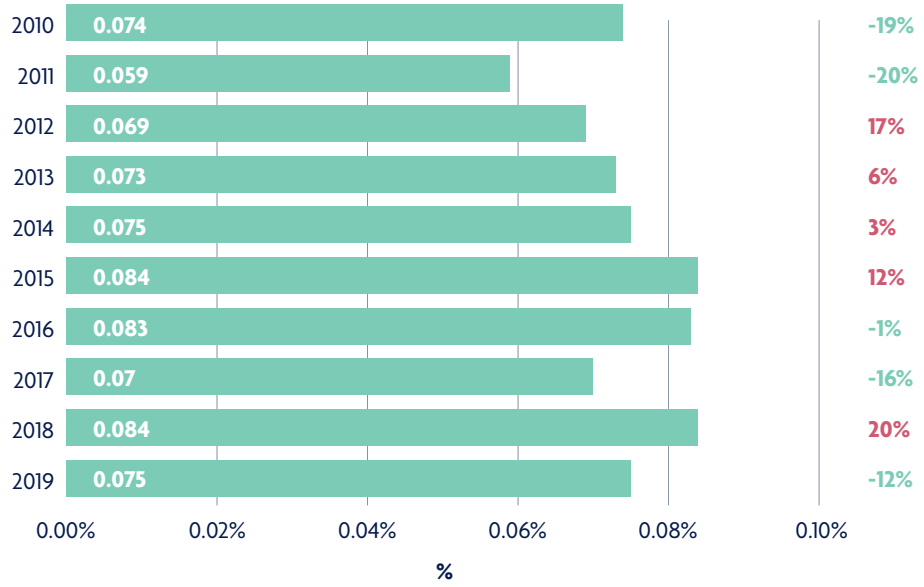
UK Finance also publishes the number of fraud incidents to convey more fully the dynamics of the fraud environment in the UK. Whilst losses have been decreasing, the number of confirmed cases has increased during the same period, rising by five per cent to 2,745,539 cases. This demonstrates that cases are being spotted and stopped by card issuers more quickly, with a lower average loss per case (£381 in 2010 down to £226 in 2019).

There was a rise in the number of cases involving remote purchase fraud and lost and stolen cards in 2019, which has driven the overall rise in fraud volumes.

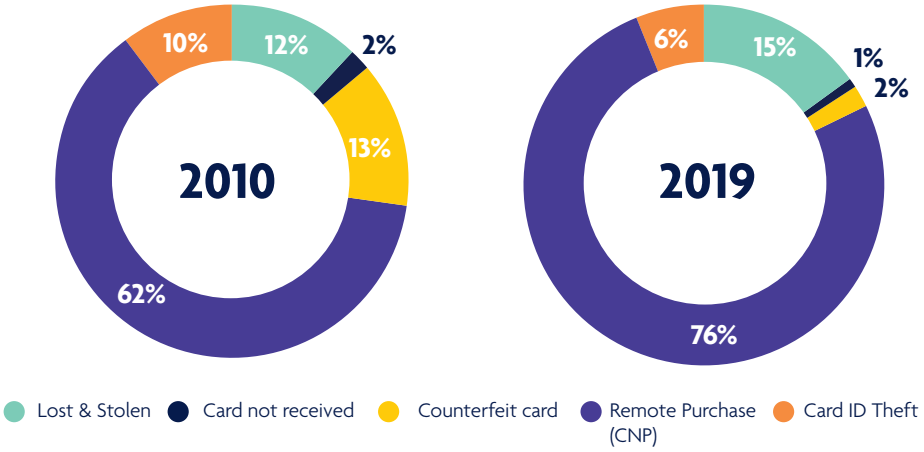
It is important to note that the number of cases relates to the number of accounts that have been defrauded, as opposed to the number of victims.

Card Fraud Type on UK-issued credit and debit cards	2015	2016	2017	2018	2019	% Change 18/19
Remote Purchase (CNP)	1,113,084	1,437,832	1,398,153	2,050,275	2,157,418	5%
Counterfeit (skimmed/cloned)	86,021	108,597	85,025	58,636	65,907	12%
Fraud on lost or stolen cards	143,802	231,164	350,279	434,991	460,142	6%
Card ID theft	33,566	31,756	29,156	63,791	54,165	-15%
Card non-receipt	10,719	11,377	10,903	10,046	7,907	-21%
Total	**1,387,192**	**1,820,726**	**1,873,516**	**2,617,739**	**2,745,539**	**5%**

Fraud to turnover ratio 2010 – 2019



Card fraud losses 2019 split by type (as a percentage of total losses)



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

VALUE	£470.2m	-7%

VOLUME	2,157,418	+5%

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 dropped to £470.2 million in 2019; a decrease of seven per cent when compared to 2018. Online fraud against UK retailers totalled an estimated £239.9 million in 2019, a decrease of ten per cent on the previous year. Mail and telephone order (MOTO) fraud against retailers based in the UK also decreased, falling five per cent to £87.3 million.

The increase in the number of cases of remote purchase fraud of five per cent, compared with the decrease in gross losses of seven per cent, suggests that card issuers are identifying and stopping individual incidents more quickly.

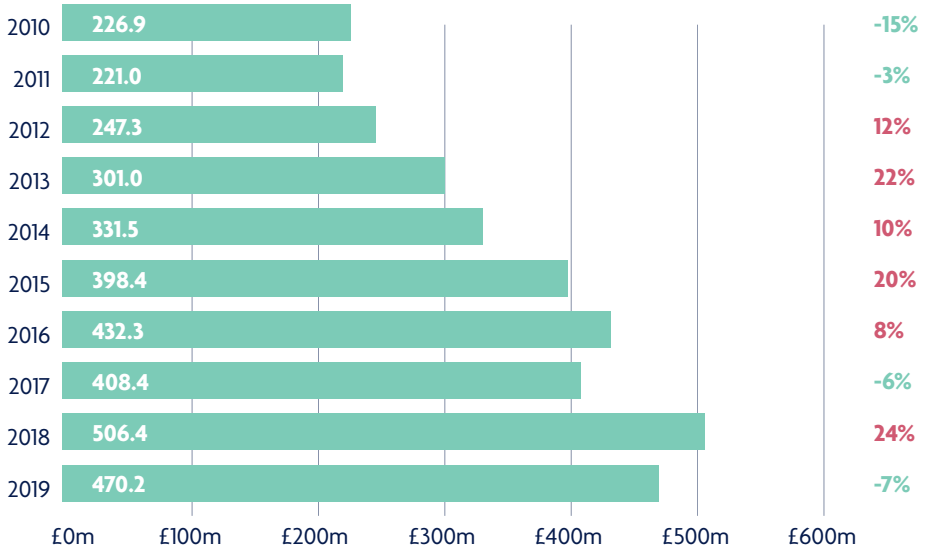
Intelligence suggests that this type of fraud results mainly from the criminal use of card details that have been obtained through data compromise, including third-party data breaches, phishing emails and scam text messages. There have been a number of high-profile data breaches affecting UK cardholders in 2019, as well as lower profile attacks, with criminals using the stolen data to make unauthorised purchases online, in particular.

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 stolen card details to purchase the item from a legitimate source and then keeps the payment from the customer.

More than 1,600 social media accounts linked to scam activity were taken down last year following the work of the DCPCU, a specialist fraud squad funded by the banking and finance industry, which has been working with social media platforms to identify accounts which feature posts relating to payment crime.

More than 400 of the accounts removed were so-called "brokers", who advertise goods and services at reduced prices that have been bought using stolen card details.

Remote purchase (CNP) fraud losses on UK-issued cards 2010 – 2019



How to stay safe from remote purchase fraud:

- If you're using an online retailer for the first time, always take time to research them before you give them any of your details. Be prepared to ask questions before making a payment.
- If an offer looks too good to believe then it probably is. Be suspicious of prices that are unfeasibly low.
- 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

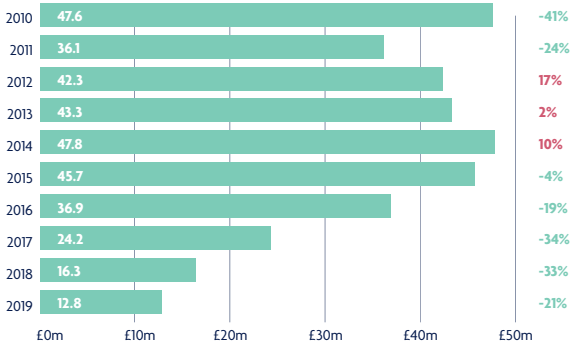
VALUE	£12.8m	-21%

VOLUME	65,907	+12%

This fraud occurs when a criminal creates a fake card using information obtained from the magnetic stripe.

Counterfeit card losses totalled £12.8 million in 2019, a decrease of 21 per cent compared to 2018 and 92 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. However, there has been an increase in attempts by fraudsters in other parts of the world where Chip and PIN has not been adopted to use counterfeit cards for financial advantage.

Counterfeit card fraud losses on UK-issued cards 2010 – 2019



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

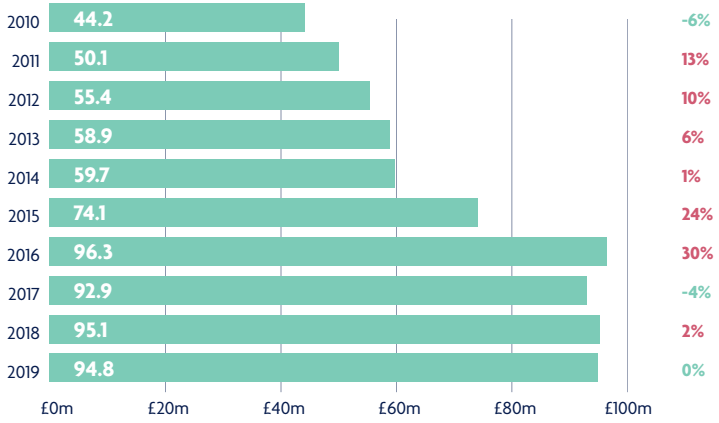
VALUE	£94.8m	0%

VOLUME	460,142	+6%

This fraud occurs when a criminal uses a lost or stolen card to make a purchase or payment (whether remotely or face-to-face) or takes money out at an ATM or in a branch.

Losses due to lost and stolen fraud slightly decreased in 2019, falling to £94.8 million. However, the number of incidents increased by six 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. In March 2020, new rules (the EU's second Payment Services Directive (PSD2)) came into force which means customers now have to enter their PIN once their 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 2010 – 2019



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 or wallet whenever you enter it.
- If you spot anything suspicious with an ATM, or someone is watching you, then do not use the machine and report it to your bank.

Card ID theft

VALUE	£37.7m	-20%

VOLUME	54,165	-15%

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 decreased by 20 per cent in 2019 to £37.7 million, with the number of cases decreasing by 15 per cent to 54,165. 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 mailboxes and multi-occupancy buildings.

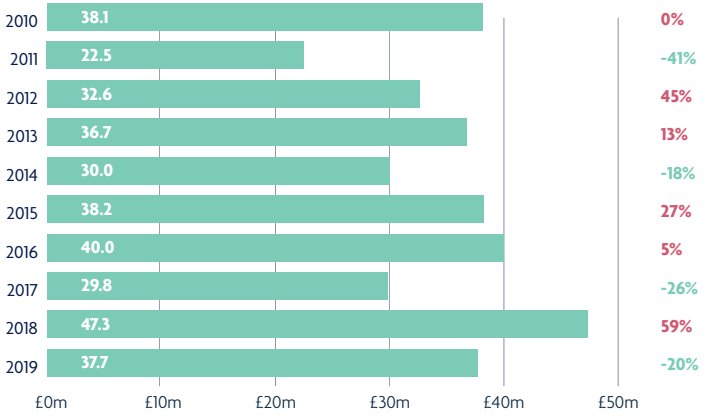
Application fraud – £17.4 million (-41%)

Application fraud occurs when criminals use stolen or fake documents to open an account in someone else's name. For identification 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 - £20.3 million (+13%)

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.

ID theft on UK-issued cards 2010 – 2019



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 report 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	£5.2m	-17%

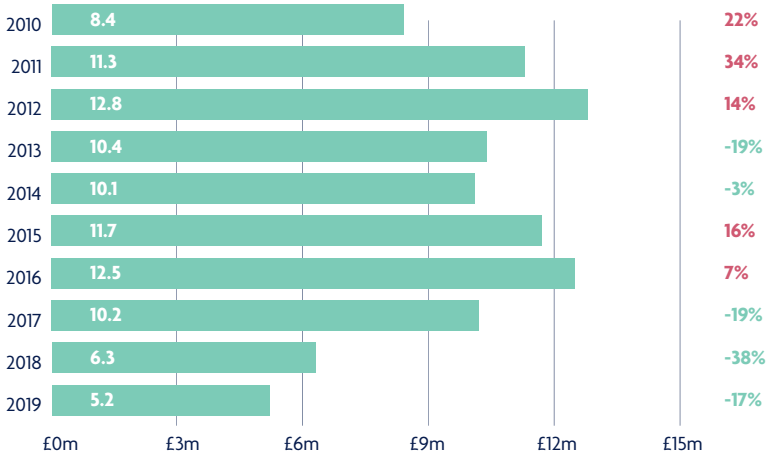
VOLUME	7,907	-21%

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 17 per cent in 2019 to £5.2 million.

Criminals typically target properties with communal letterboxes, such as flats and student halls of residence, and external mailboxes 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 2010-2019



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 or building society.

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	£ 64.3m	-8%

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 decreased eight per cent in 2019 to £64.3 million.

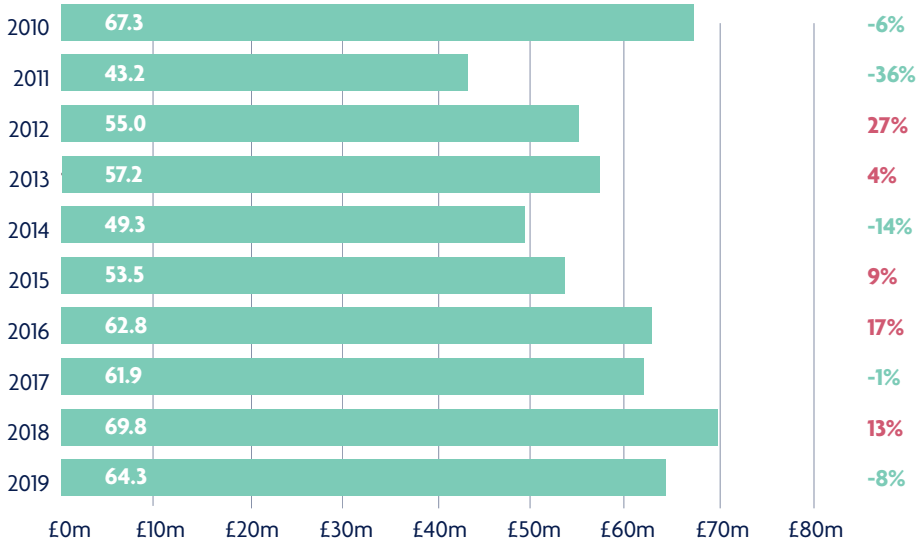
The majority of this fraud is undertaken using low-tech techniques, with fraudsters finding ways of stealing the card, and often the PIN, to carry out fraudulent transactions in shops. This includes criminals using methods such as ATM card entrapment and distraction thefts, combined with shoulder surfing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

This category includes fraud incidents involving the contactless functionality on both payment cards and mobile devices. Contactless fraud on payment cards and devices remains low with £20.6 million of losses during 2019, compared to spending of £80.5 billion over the same period.

This is equivalent to 2.5p in every £100 spent using contactless technology, a reduction in the total recorded in 2018 (2.7p). Contactless fraud on payment cards and devices represents just 3.3 per cent of overall card fraud losses, while 44 per cent of all card transactions were contactless last year.

Each 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 varies between card issuers. In September of last year new rules (the EU's second Payment Services Directive (PSD2)) came into play which now require a PIN once a customer's total 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) 2010-2019



Internet/e-commerce fraud

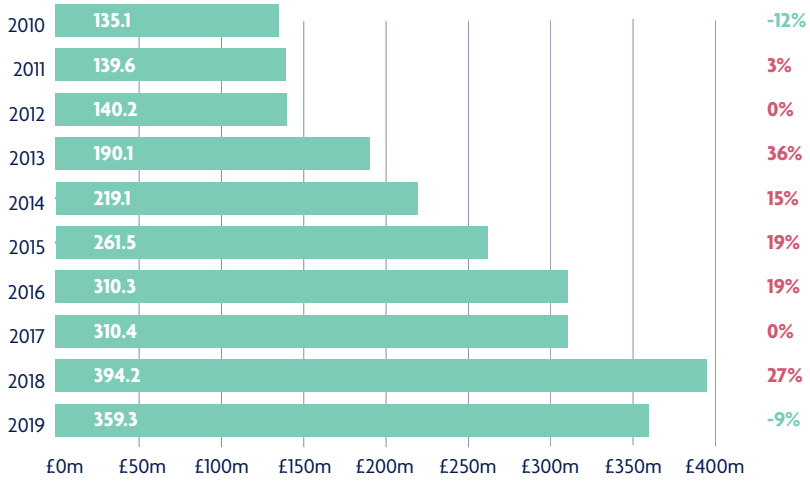
VALUE	£359.3 m	-9%

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 £359.3 million of e-commerce fraud took place on cards in 2019, accounting for 58 per cent of all card fraud and 76 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 2019, 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 during 2019 were £309 billion, meaning that for every £100 spent online only 15pence was fraudulent.

Internet/e-commerce fraud losses on UK issued cards 2010-2019



Card fraud at UK cash machines

VALUE	£30.0m	-8%

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, or from distraction thefts in shops and bars.

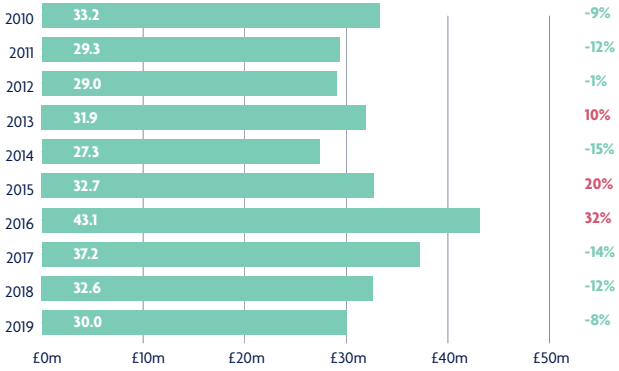
Fraudsters also target cash machines to compromise or steal cards or card details in three main ways:

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 and 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 2010-2019



Card fraud abroad

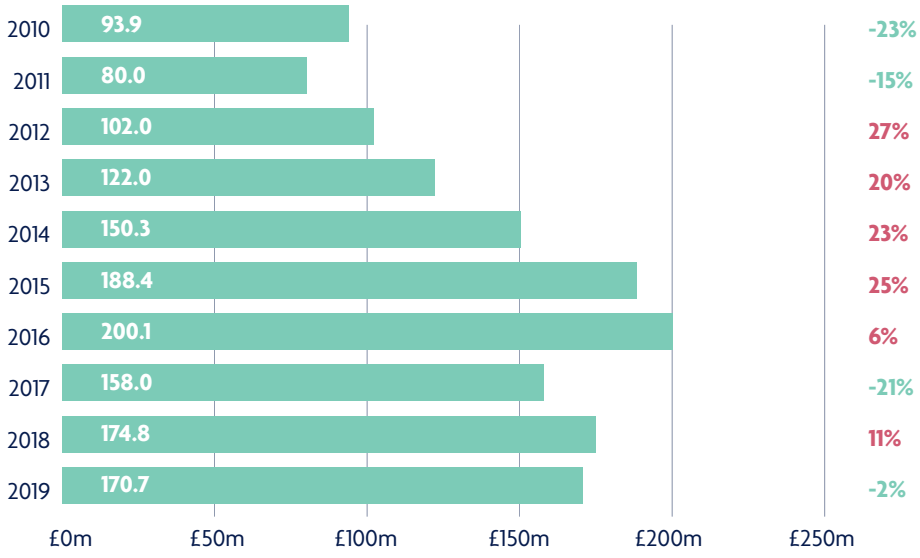
VALUE	£170.7m	-2%

This category covers fraud occurring in locations overseas on UK-issued cards. The majority (86 per cent) of this type of fraud is attributed to remote purchase fraud at overseas retailers.

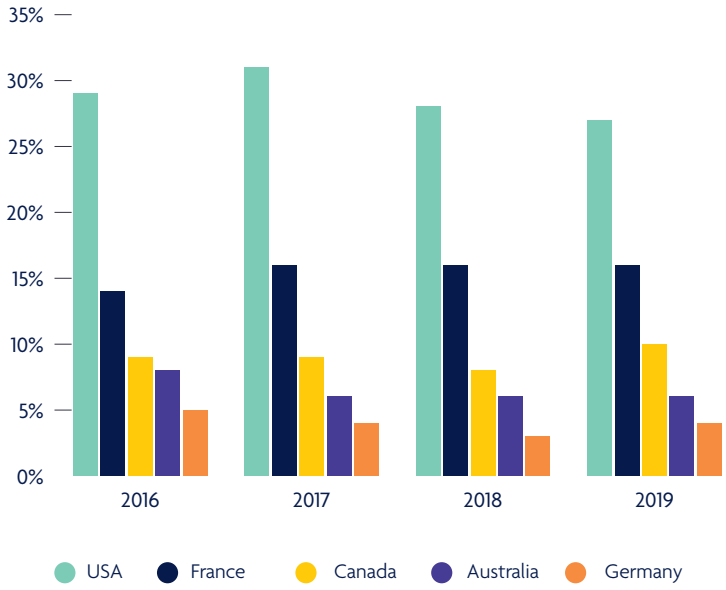
This category also includes cases where criminals steal the magnetic stripe details from UK-issued cards to make counterfeit cards which are used overseas in countries yet to upgrade to Chip and PIN.

International fraud losses for 2019 were £170.7 million, compared with losses at their peak in 2008 of £230.1 million, a decrease of 26 per cent.

Fraud committed abroad on UK-issued cards 2010-2019

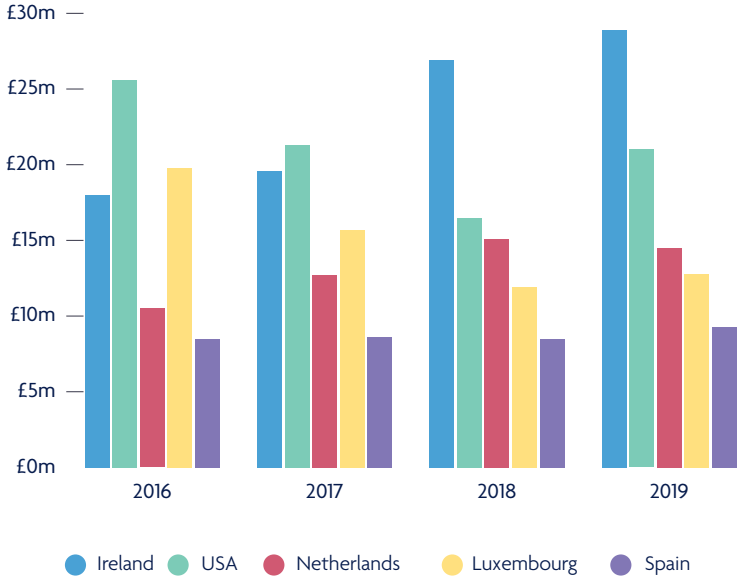


Top five countries for fraud on foreign-issued cards occuring in the UK 2016-2019 (%)



Top five countries where fraud on UK-issued cards occurs 2016-2019 (£m)

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



CHEQUE FRAUD

Cheque fraud

VALUE	£53.6m	+161%

VOLUME	2,852	+41%

Cheque fraud losses increased to £53.6 million in 2019. The volume of fraudulent cheques increased by only 41 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.

Intelligence suggests the increase was largely a result of fraudsters targeting high-value corporate accounts, where losses per case are typically far higher than on individual customer accounts. Personal customers only accounted for a small fraction of the total losses. This raises the question of whether large firms need to enhance the security features on cheques to deter fraudsters. It also reflects better awareness among consumers of the risks of fraud, due in large part to industry-led educational campaigns. A total of £550.8 million of cheque fraud was prevented in 2019, up by 152 per cent on 2018. This is equivalent to £9.11 in every £10 of attempted cheque fraud being stopped before a loss occurs. This remains the highest proportion of attempted fraud stopped across all the fraud types. There are three types of cheque fraud: counterfeit, forged and fraudulently altered.

Counterfeit cheque fraud - £41.3 million (+159%)

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 - £6.4 million (+88%)

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

Fraudulently altered cheques - £5.9 million (+379%)

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.

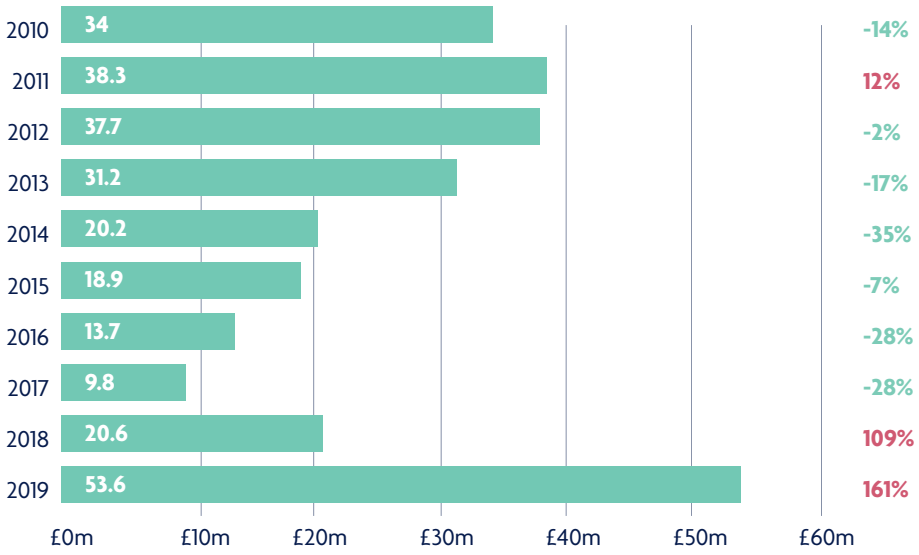
Prevented cheque fraud 2015 - 2019

Year	2015	2016	2017	2018	2019	18/19 % Change
Cheque Fraud	£392.8m	£196.2m	£212.3m	£218.2m	£550.8m	152%

Annual case volumes cheque fraud 2015-2019

Year	2015	2016	2017	2018	2019	18/19 % Change
Cheque Fraud	5,746	3,388	1,745	2,020	2,852	41%

Cheque Fraud losses 2010-2019



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	£150.7m	-1%	VOLUME	43,906	+38%

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 £150.7 million in 2019, one per cent lower than compared to 2018. The number of cases of remote banking fraud increased by 38 per cent to 43,906. This reflects the greater number of people now regularly using internet, telephone and mobile banking, and attempts by fraudsters to take advantage of this. In 2019, 81 per cent of the adult population used at least one form of remote banking.

A total of £268.8 million of attempted remote banking fraud was stopped by bank security systems during 2019. This is equivalent to £6.41 in every £10 of fraud attempted being prevented. In addition, 17 per cent (£25.8 million) of the losses across all remote banking channels were recovered after the incident.

Case volumes were not collected until 2012.

Remote Banking Fraud losses 2012-2019

Remote banking values	2012	2013	2014	2015	2016	2017	2018	2019	Change
Internet banking	£57.0m	£58.8m	£81.4m	£133.5m	£101.8m	£121.2m	£123.0m	£111.8m	-9%
Telephone banking	£14.7m	£13.1m	£16.8m	£32.3m	£29.6m	£28.4m	£22.0m	£23.6m	7%
Mobile banking	N/A	N/A	N/A	£2.8m	£5.7m	£6.5m	£7.9m	£15.2m	94%
TOTAL	**£71.7m**	**£71.9m**	**£98.2m**	**£168.6m**	**£137.0m**	**£156.1m**	**£152.9m**	**£150.7m**	**-1%**

Annual case volumes Remote Banking fraud 2012-2019

Remote banking cases	2012	2013	2014	2015	2016	2017	2018	2019	Change
Internet banking	16,355	13,799	16,041	19,691	20,088	21,745	20,904	25,849	24%
Telephone banking	7,095	5,596	5,778	11,380	10,495	9,577	7,937	11,185	41%
Mobile banking	N/A	N/A	N/A	2,235	2,809	3,424	2,956	6,872	132%
Total	**23,450**	**19,395**	**21,819**	**33,306**	**33,392**	**34,746**	**31,797**	**43,906**	**38%**

The finance industry is tackling remote banking fraud by:

- Continuously investing in advanced security systems, including sophisticated ways of authenticating customers, such as using biometrics and customer behaviour analysis.
- Providing customers with free security software, which many banks offer.
- Investing in the **Take Five to Stop Fraud** campaign to educate customers on how they can protect themselves from fraud and scams.
- Sharing intelligence and information on this type of fraud so that security systems can be adapted to stop the latest threats.
- Working with law enforcement, the government, the telecommunications industry and others to further improve security and to identify and prosecute the criminals responsible.

Internet banking fraud

VALUE	£111.8m	-9%

VOLUME	25,849	+24%

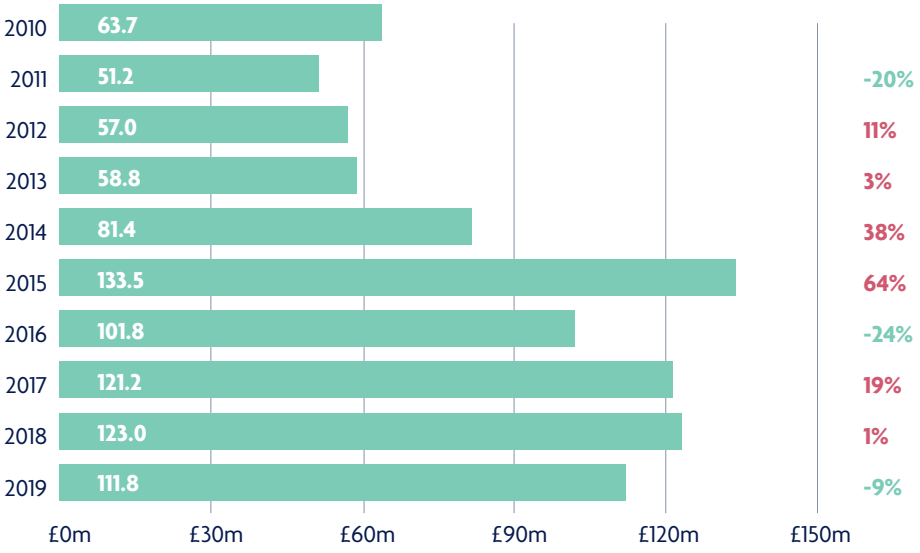
This type of fraud occurs when a fraudster gains access to a customer's online bank account and makes an unauthorised transfer of money.

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.

A total of £215.2 million of attempted internet banking fraud was stopped by bank security systems during 2019. This is equivalent to £6.58 in every £10 of fraud attempted being prevented. In addition, 20 per cent (£22.4 million) of the losses across the internet banking channel were recovered after the incident.

Case volumes were not collected until 2012.

Internet banking fraud losses 2010-2019



Annual case volumes for internet banking fraud 2012-2019

	2012	2013	2014	2015	2016	2017	2018	2019	Change
Internet banking fraud	16,355	13,799	16,041	19,691	20,088	21,745	20,904	25,849	24%

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	£23.6m	+7%

VOLUME	11,185	+41%

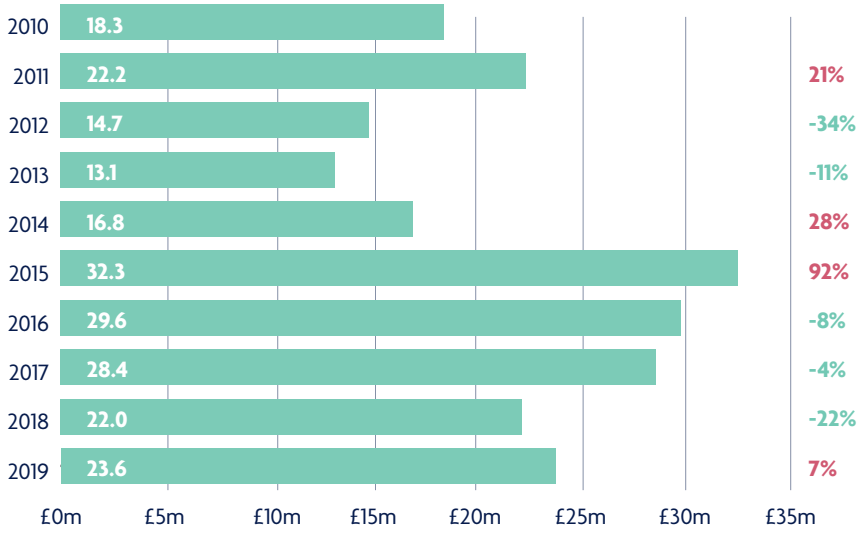
This type of fraud occurs when a criminal gains access to the victim's telephone banking account and makes an unauthorised transfer of money away from it.

Similar to internet 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.

A total of £42.2 million of attempted telephone banking fraud was stopped by bank security systems during 2019. This is equivalent to £6.41 in every £10 of fraud attempted being prevented. In addition, nine per cent (£2.1 million) of the losses across the telephone banking channel were recovered after the incident.

Case volumes were not collected until 2012.

Telephone banking fraud losses 2010-2019



Annual case volumes for telephone banking fraud 2012-2019

	2012	2013	2014	2015	2016	2017	2018	2019	Change
Telephone banking fraud	7,095	5,596	5,778	11,380	10,495	9,577	7,937	11,185	41%

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	£15.2m	+94%

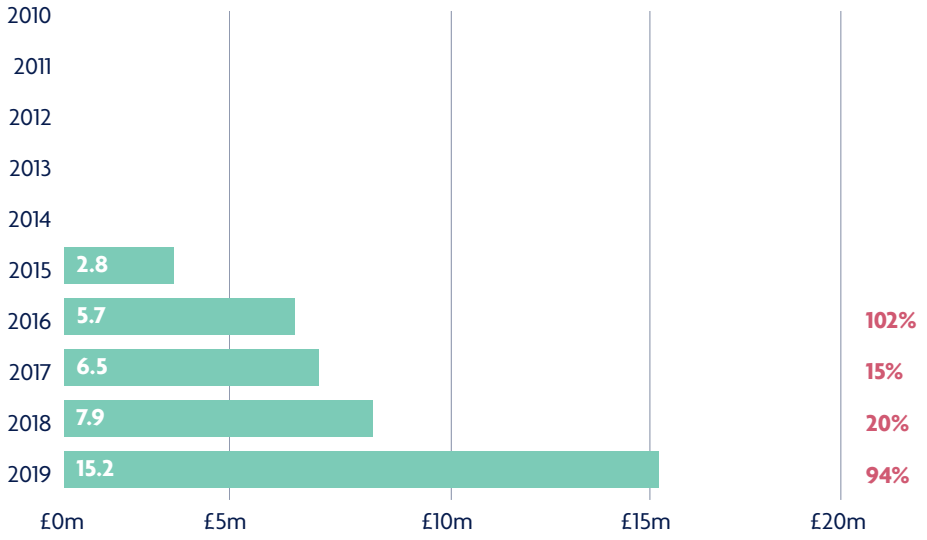
VOLUME	6,872	+132%

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. 50 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.

A total of £11.5 million of attempted mobile banking fraud was stopped by bank security systems during 2019. This is equivalent to £4.31 in every £10 of fraud attempted being prevented. In addition, eight per cent (£1.3 million) of the losses across the mobile banking channel were recovered after the incident.

Mobile banking fraud losses 2010-2019



Annual case volumes for mobile banking fraud 2012-2019

	2012	2013	2014	2015	2016	2017	2018	2019	Change
Mobile banking fraud	N/A	N/A	N/A	2,235	2,809	3,424	2,956	6,872	132%

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	£455.8m	+29%

VOLUME	122,437	+45%

UK Finance began collating and publishing data on authorised push payment (APP) scams (also known as bank transfer 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.

- In January 2018, UK Finance introduced new best practice standards for banks and building societies when responding to APP scam claims. This has greatly improved the identification and reporting processes.
- In May of last year the APP scams voluntary Code was launched. It provides customers of the nine signatory banks with greater protection against APP fraud. The introduction of the Code is thought to have driven up the number of people reporting APP scams.

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 £455.8 million in 2019. This was split between personal (£317.1 million) and non-personal or business (£138.7 million).

In total there were 122,437 cases relating to a total of 121,658 victims. Of this total, 114,731 cases were on personal accounts and 7,706 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.

APP fraud losses continue to be driven by the abuse of online platforms used by criminals to scam their victims. These include investment scams advertised on search engines and social media, romance scams committed via online dating platforms and purchase scams promoted through auction websites. 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.

All APP cases reported 2018 - 2019

		PERSONAL			NON PERSONAL			TOTAL		
		2018	2019	% Change	2018	2019	% Change	2018	2019	% Change
Volume	Cases	78,215	114,731	47%	6,409	7,706	20%	84,624	122,437	45%
	Payments	114,707	174,798	52%	8,950	10,651	19%	123,657	185,449	50%
Value	Value	£228.4m	£317.1m	39%	£126.0m	£138.7m	10%	£354.3m	£455.8m	29%
	Reimbursed	£42.3m	£82.2m	94%	£40.3m	£33.8m	-16%	£82.6m	£116.0m	40%

APP Voluntary Code statistics

As stated above, on 28 May 2019, following work between the industry, consumer groups and the regulator, the authorised push payment (APP) scams voluntary code was introduced. It provides protections for customers of signatory payment service providers (PSPs) and delivers a significant commitment from all signatory firms to reimburse victims of authorised push payment fraud in any scenario where the customer has met the standards expected of them under the code.

For the first time UK Finance is publishing statistics relating to the cases assessed using the voluntary code and the compensation provided to customers. This data covers the period 28 May 2019 to 31 December 2019. It shows that 50,311 cases have been assessed and closed since the code was introduced, with a total value of £101.1 million. Of this, £41.3 million was reimbursed to victims, accounting for 41 per cent of total losses in these cases. This is a significant increase on the proportion reimbursed before the code was introduced (19 per cent Jan to June 2019).

Of the 50,311 cases reported, 75 per cent involved values of less than £1,000. Four per cent of cases involved more life-changing sums of £10,000 plus. Reimbursement rates were higher for fraud cases involving losses of £10,000 or more, and for impersonation scams in which criminals imitate the police, banks or other organisations.

Cases assessed using the voluntary code by signatory PSPs (28 May 2019 to 31 December 2019)

All cases reported below are included in previous figures relating to all APP cases reported and should not be treated as an addition.

		Less than £1k	£1k - £10k	More than £10k	Total
Volume	**Cases**	37,795	10555	1961	**50,311**
	Payments	45,569	18137	4841	**68,547**
Value	**Value**	10.4m	36.4m	54.2m	**101.1m**
	Reimbursed	3.4m	14.7m	23.1m	**41.3m**

The finance industry is tackling authorised push payment scams by:

- The implementation of the industry-wide APP scams voluntary code which helps to improve protections and reimburse many victims of these scams.
- Helping to prevent customers being duped by criminals by raising awareness of scams and how to stay safe through the Take Five and Don't Be Fooled campaigns.
- Delivering the Banking Protocol – a ground-breaking rapid response scheme through which branch staff can alert police and Trading Standards to suspected frauds taking place. The system is now operational in every police force area and has prevented £96.6 million in fraud and led to 643 arrests since launching in March 2017.
- 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 2019 the Unit prevented an estimated £31.2 million of fraud, secured 75 convictions and disrupted 34 organised crime groups.
- Working with Pay.UK to implement Mule Insights Tactical Solution (MITS), a new technology that helps to track suspicious payments and identify money mule accounts.
- 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.

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).
- **Six payment types:** Faster Payment, 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.

Included within each scam type is the data relating to the cases which have been assessed using the voluntary reimbursement code introduced in May 2019.

SCAM TYPES

Malicious payee

Purchase scams

VALUE	£59.0m	+27%	VOLUME	73,336	+39%

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 2019, with the 73,336 cases accounting for 60 per cent of the total number of APP scam cases. A total of £59 million was lost to purchase scams in 2019, with the vast majority of losses being from personal accounts. Payment service providers were subsequently able to return £9.7 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.

All Purchase scam cases reported 2018 – 2019

		PERSONAL			NON PERSONAL			TOTAL		
		2018	2019	% Change	2018	2019	% Change	2018	2019	% Change
Volume	Cases	51,208	71,574	40%	1,413	1,762	25%	52,621	73,336	39%
	Payments	65,033	90,942	40%	1,663	2,178	31%	66,696	93,120	40%
Value	Value	£42.4m	£51.1m	20%	£4.0m	£7.9m	99%	£46.4m	£59.0m	27%
	Reimbursed	£3.8m	£8.9m	136%	£0.5m	£0.8m	78%	£4.2m	£9.7m	129%

Cases assessed using the voluntary code by signatory PSPs (28 May 2019 to 31 December 2019)

All cases reported below are included in previous figures relating to all purchase scam cases reported and should not be treated as an addition.

		Less than £1k	£1k - £10k	More than £10k	Total
Volume	**Cases**	24,832	3,066	191	**28,089**
	Payments	29,323	4,657	474	**34,454**
Value	**Value**	£5.6m	£9.0m	£3.8m	**£18.4m**
	Reimbursed	£1.4m	£2.6m	£0.9m	**£4.9m**

For those cases which were applicable for assessment using the voluntary code, 27 per cent of all losses were refunded to the victim. However, this is an increase from the ten per cent being reimbursed in the six months before the code was introduced (December 2018 to May 2019).

88 per cent of all cases assessed involved case values of less than £1,000.

How to stay safe from purchase scams:

- Be suspicious of any 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	£ 95.4m	+90%	VOLUME	6,789	+101%

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 usually promise a high return in order to entice their victim into making the transfer. These scams include investment 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. FCA analysis suggests that the rise in investment fraud is being driven in part by criminals targeting consumers online, for example through adverts on search engines or social media channels

A total of £95.4 million was lost to investment scams in 2019, with payment services providers subsequently able to return £12.3 million. The nature of the scams means that the sums involved in individual cases can be higher, so while investment scams accounted for only six per cent of the total number of APP scam cases, they accounted for 21 per cent of the total value.

All investment scam cases reported 2018 - 2019

		PERSONAL			NON PERSONAL			TOTAL		
		2018	2019	% Change	2018	2019	% Change	2018	2019	% Change
Volume	Cases	3,312	6,679	102%	73	110	51%	3,385	6,789	101%
	Payments	7,795	13,962	79%	141	261	85%	7,936	14,223	79%
Value	Value	£48.5m	£89.5m	84%	£1.6m	£5.9m	264%	£50.1m	£95.4m	90%
	Reimbursed	£3.7m	£11.7m	218%	£0.2m	£0.6m	154%	£3.9m	£12.3m	214%

Cases assessed using the voluntary code by signatory PSPs (28 May 2019 to 31 December 2019)

All cases reported below are included in previous figures relating to all investment scam cases reported and should not be treated as an addition

		Less than £1k	£1k - £10k	More than £10k	Total
Volume	**Cases**	1,090	583	356	**2,029**
	Payments	1,585	1,125	860	**3,570**
Value	**Value**	£0.6m	£2.1m	£13.5m	**£16.2m**
	Reimbursed	£0.3m	£0.5m	£4.0m	**£4.8m**

For only those cases which were applicable for assessment using the voluntary code, 29 per cent of all losses were repatriated to the victim; in the six months before the code was introduced (December 2018 to May 2019) just seven per cent was reimbursed.

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 investments 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.
- Be wary of investment adverts which come up on search engines.

Romance scams

VALUE	£18.1m	+43%	VOLUME	2,163	+54%

In a romance scam, the victim is persuaded 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 £18.1 million was lost to romance scams in 2019. 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 2019 and four per cent of the total value. Payment service providers were only able to return £2.4 million 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.

All romance scam cases reported 2018 - 2019

		PERSONAL			NON PERSONAL			TOTAL		
		2018	2019	% Change	2018	2019	% Change	2018	2019	% Change
Volume	Cases	1,400	2,137	53%	4	26	550%	1,404	2,163	54%
	Payments	7,557	10,956	45%	17	61	259%	7,574	11,017	45%
Value	Value	£12.5m	£18.0m	44%	£0.1m	£0.1m	-10%	£12.6m	£18.1m	43%
	Reimbursed	£0.6m	£2.3m	265%	£0.0m	£0.0m	2884%	£0.6m	£2.4m	267%

Cases assessed using the voluntary code by signatory PSPs (28 May 2019 to 31 December 2019)

All cases reported below are included in previous figures relating to all romance scam cases reported and should not be treated as an addition

		Less than £1k	£1k - £10k	More than £10k	Total
Volume	**Cases**	361	308	94	**763**
	Payments	725	1,489	768	**2,982**
Value	**Value**	£0.1m	£1.2m	£2.5m	**£3.8m**
	Reimbursed	£0.0m	£0.3m	£0.6m	**£0.9m**

For only those cases which were applicable for assessment using the voluntary code, 25 per cent of all losses were returned to the victim. In the six months before the code was introduced (December 2018 to May 2019) only six per cent was reimbursed.

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. Check if the photo has been used elsewhere.
- Contact your bank straight away if you think you may have fallen victim to a romance scam.

Advance fee scams

VALUE	£17.2m	+23%

VOLUME	10,711	+32%

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 third most common form of APP scam in 2019, accounting for nine per cent of the total number of cases. A total of £17.2 million was lost to advance fee scams last year, meaning by value these scams accounted for four per cent of all APP scams.

All advance fee scam cases reported 2018 - 2019

		PERSONAL			NON PERSONAL			TOTAL		
		2018	2019	% Change	2018	2019	% Change	2018	2019	% Change
Volume	Cases	7,915	10,508	33%	218	203	-7%	8,133	10,711	32%
	Payments	12,876	16,828	31%	395	276	-30%	13,271	17,104	29%
Value	Value	£12.8m	£16.0m	25%	£1.2m	£1.3m	7%	£14.0m	£17.2m	23%
	Reimbursed	£1.1m	£2.1m	96%	£0.3m	£0.1m	-46%	£1.4m	£2.3m	68%

Cases assessed using the voluntary code by signatory PSPs (28 May 2019 to 31 December 2019)

All cases reported below are included in previous figures relating to all advance fee scam cases reported and should not be treated as an addition

		Less than £1k	£1k - £10k	More than £10k	Total
Volume	Cases	3,774	955	78	4,807
	Payments	5,150	1,776	222	7,148
Value	Value	£1.2m	£2.4m	£1.9m	£5.5m
	Reimbursed	£0.3m	£0.6m	£0.5m	£1.4m

For only those cases which were applicable for assessment using the voluntary code, 25 per cent of all losses were returned to the victim. In the six months before the code was introduced (December 2018 to May 2019) only eight per cent was reimbursed.

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	£114.1m	-8%	VOLUME	8,572	+13%

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 only the fourth most common type of APP scam in 2019. However, they resulted in the largest share of losses at 25 per cent, totalling £114.1 million. The majority of losses by value, some £82.4 million, were from non-personal or business accounts, where the average payment was £16,209. This reflects the fact that businesses make higher-value payments more regularly.

All invoice and mandate scam cases reported 2018 - 2019

		PERSONAL			NON PERSONAL			TOTAL		
		2018	2019	% Change	2018	2019	% Change	2018	2019	% Change
Volume	Cases	4,274	4,732	11%	3,280	3,840	17%	7,554	8,572	13%
	Payments	5,431	6,387	18%	4,467	5,081	14%	9,898	11,468	16%
Value	Value	£31.0m	£31.7m	2%	£92.7m	£82.4m	-11%	£123.7m	£114.1m	-8%
	Reimbursed	£6.8m	£12.8m	88%	£29.6m	£19.5m	-34%	£36.4m	£32.3m	-11%

Cases assessed using the voluntary code by signatory PSPs (28 May 2019 to 31 December 2019)

All cases reported below are included in previous figures relating to all invoice and mandate scam cases reported and should not be treated as an addition

		Less than £1k	£1k - £10k	More than £10k	Total
Volume	Cases	660	1202	326	2188
	Payments	727	1356	440	2523
Value	Value	0.6m	5.6m	11.7m	17.9m
	Reimbursed	0.2m	2.2m	5.5m	7.9m

For only those cases which were applicable for assessment using the voluntary code, 44 per cent of all losses were returned to the victim. In the six months before the code was introduced (December 2018 to May 2019) only 24 per cent was reimbursed.

How to stay safe from invoice and mandate scams:

- Always confirm any bank account details directly with the genuine 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. If you receive an email telling you to change payment details 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	£17.8m	+20%	VOLUME	676	+12%

CEO fraud is where the scammer manages to impersonate the CEO or other high ranking official 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 2019, accounting for less than one per cent of total cases. A total of £17.8 million was lost, equivalent to four per cent of the total case value.

All CEO fraud scam cases reported 2018 - 2019

		PERSONAL			NON PERSONAL			TOTAL		
		2018	2019	% Change	2018	2019	% Change	2018	2019	% Change
Volume	Cases	84	80	-5%	519	596	15%	603	676	12%
	Payments	99	153	55%	732	809	11%	831	962	16%
Value	Value	£1.0m	£1.2m	18%	£13.8m	£16.5m	20%	£14.8m	£17.8m	20%
	Reimbursed	£0.2m	£0.3m	110%	£4.2m	£3.5m	-15%	£4.3m	£3.9m	-10%

Cases assessed using the voluntary code by signatory PSPs (28 May 2019 to 31 December 2019)

All cases reported below are included in previous figures relating to all CEO fraud scam cases reported and should not be treated as an addition

		Less than £1k	£1k - £10k	More than £10k	Total
Volume	Cases	6	48	23	77
	Payments	6	63	32	101
Value	Value	£0.0m	£0.2m	£0.4m	£0.7m
	Reimbursed	£0.0m	£0.1m	£0.1m	£0.3m

For only those cases which were applicable for assessment using the voluntary code, 40 per cent of all losses were refunded to the victim; in the six months before the code was introduced (December 2018 to May 2019) only 26 per cent was reimbursed.

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	£84.1m	+49%	VOLUME	11,088	+103%

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 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 nine per cent of all APP scam cases in 2019. £84.1 million was lost due to these scams, which by value was the third highest type of APP scam, accounting for 18 per cent of total losses. Payment service providers were able to return £37.3 million of the losses to customers.

All police/bank impersonation scam cases reported 2018 - 2019

		PERSONAL			NON PERSONAL			TOTAL		
		2018	2019	% Change	2018	2019	% Change	2018	2019	% Change
Volume	Cases	5,112	10,835	112%	347	253	-27%	5,459	11,088	103%
	Payments	7,996	21,606	170%	707	654	-7%	8,703	22,260	156%
Value	Value	£49.8m	£73.5m	48%	£6.7m	£10.7m	60%	£56.5m	£84.1m	49%
	Reimbursed	£16.8m	£29.6m	76%	£3.1m	£7.8m	154%	£19.8m	£37.3m	88%

Cases assessed using the voluntary code by signatory PSPs (28 May 2019 to 31 December 2019)

All cases reported below are included in previous figures relating to all impersonation scam cases reported and should not be treated as an addition

		Less than £1k	£1k - £10k	More than £10k	Total
Volume	Cases	1,440	2,602	627	4,669
	Payments	1,759	4,431	1,330	7,520
Value	Value	£0.8m	£9.8m	£12.9m	£23.5m
	Reimbursed	£0.5m	£5.5m	£6.4m	£12.4m

For only those cases which were applicable for assessment using the voluntary code, 53 per cent of all losses were refunded to the victim; the second highest of all eight scam types. In the six months before the code was introduced (December 2018 to May 2019) only 26 per cent was reimbursed.

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	£50.2m	+39%	VOLUME	9,102	+67%

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 £50.2 million was lost to this type of scam in 2019, with payment service providers subsequently able to return £15.9 million. Impersonation: other scams accounted for seven per cent of all APP scam cases last year, representing 11 per cent of total losses.

All other impersonation scam cases reported 2018 - 2019

		PERSONAL			NON PERSONAL			TOTAL		
		2018	2019	% Change	2018	2019	% Change	2018	2019	% Change
Volume	Cases	4,910	8,186	67%	555	916	65%	5,465	9,102	67%
	Payments	7,920	13,964	76%	828	1,331	61%	8,748	15,295	75%
Value	Value	£30.3m	£36.2m	20%	£6.0m	£14.0m	136%	£36.2m	£50.2m	39%
	Reimbursed	£9.4m	£14.5m	54%	£2.5m	£1.4m	-44%	£11.9m	£15.9m	33%

Cases assessed using the voluntary code by signatory PSPs (28 May 2019 to 31 December 2019)

All cases reported below are included in previous figures relating to all other impersonation scam cases reported and should not be treated as an addition

		Less than £1k	£1k - £10k	More than £10k	Total
Volume	Cases	2,105	1,791	266	4,162
	Payments	2,767	3,240	715	6,722
Value	Value	£1.1m	£6.1m	£7.4m	£14.7m
	Reimbursed	£0.4m	£2.9m	£5.1m	£8.3m

For only those cases which were applicable for assessment using the voluntary code, 57 per cent of all losses were refunded to the victim; the highest of all eight scam types. In the six months before the code was introduced (December 2018 to May 2019) only 26 per cent was reimbursed.

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 Payment was used in 95 per cent of cases. While CHAPS was the least common payment method, representing only 0.7 per cent of cases, the high-value nature of transactions using this payment type meant that it accounted for seven per cent of the total value.

Payment type	2018	2019	% Change	2018	2019	% Change
Faster Payment	115,332	175,816	52%	£251.6m	£333.4m	32%
CHAPS	652	1,340	106%	£26.0m	£30.0m	16%
BACS	1,454	2,328	60%	£23.6m	£31.5m	34%
Intra Bank Transfer ("on us")	1,722	1,965	14%	£3.3m	£3.6m	10%
International	4,497	4,000	-11%	£49.9m	£57.4m	15%
Total	**123,657**	**185,449**	**50%**	**£354.3m**	**£455.8m**	**29%**

PAYMENT CHANNEL

This data shows the channel through which the victim made the authorised push payment. Internet banking was used in 64 per cent of cases, totalling £344.7 million of losses.

Payment type	2018	2019	% Change	2018	2019	% Change
Branch	7,919	11,072	40%	£41.3m	£49.1m	19%
Internet Banking	93,466	119,224	28%	£288.7m	£344.7m	19%
Telephone Banking	4,521	6,001	33%	£14.8m	£27.5m	85%
Mobile Banking	17,751	49,152	177%	£9.5m	£34.4m	261%
Total	**123,657**	**185,449**	**50%**	**£354.3m**	**£455.8m**	**29%**

DECISION TIMES

This data shows the amount of time between the victim reporting the authorised push payment and the date the victim is informed of the final refund decision in relation to their case. 59 per cent of cases were decided in less than a week of the case being reported.

Decision Time	2018	2019
Less than a week	65%	59%
Between week and a month	22%	27%
More than a month	14%	14%

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.

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:

Criminals are experts at impersonating people, organisations and the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment. Stop and think. It could protect you and your money.

- STOP - Taking a moment to stop and think before parting with your money or information could keep you safe.
- CHALLENGE - Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- PROTECT - Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

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

TAKE FIVE TO STOP FRAUD™


mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
elif operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True
0 10 1 0
0 10 1 0
0 10 1 0
print("please select exactly two objects, the last one get
OPERATOR CLASSES
bpy.context.scene.objects.active
Tool
0 10 1 0


0 10 1 0
0 10 1 0
print("please select exactly two objects, the
OPERATOR CLASSES