UK FINANCE

FRAUD - THE FACTS 2021

THE DEFINITIVE OVERVIEW OF PAYMENT INDUSTRY FRAUD

Sponsored by

LexisNexis®
RISK SOLUTIONS

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.

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, consumer groups 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.

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.

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 Information and Intelligence Unit and the Fraud Intelligence Sharing System (FISS) which feeds 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 national awareness campaigns (Take Five to Stop Fraud 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 for 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

2020 was a year of unprecedented challenges, as the Covid-19 pandemic dramatically transformed our everyday lives and lockdown restrictions significantly impacted on the economy.

While families and businesses have struggled, the criminal gangs behind economic crime have been quick to capitalise from the pandemic by tailoring scams to fit our changing lifestyles due to the pandemic. These include impersonation scams that seize on people's fears about the pandemic where fraudsters pretend to be from trusted organisations such as the NHS or government departments. Criminals are also adapting to the rise in online shopping and remote working by impersonating parcel delivery companies, e-commerce platforms or broadband providers. In addition, criminals are recruiting 'money mules' to launder stolen funds by posting fake adverts on job websites and social media, targeting those looking for work or to earn easy money during the pandemic.

Let's be clear, these fraudsters are not cheeky chancers, they are organised, ruthless criminals using sophisticated techniques to trick people out of their personal or financial information. As a recent report by the Royal United Services Institute (RUSI) think tank highlights, the links between fraud, organised crime and terrorism pose a significant and growing threat to our national security. The criminal gangs involved use the proceeds of fraud to fund other harmful and illegal activities such as human slavery or drugs trafficking, causing untold suffering and damage to our society. It is therefore incumbent on all of us, across the private sector, law enforcement and government, to work together to tackle this threat.

Bank staff on the frontline have been working hard throughout the pandemic to protect customers from fraud and to help the police catch the criminals responsible. The industry stopped £1.6 billion of unauthorised fraud losses in 2020, equivalent to £6.73 in every £10 of attempted fraud being stopped. The Banking Protocol, the bank branch rapid response scheme that stopped £45.3 million of scams in 2020, is now being expanded to include online and telephone banking. In addition, the banking industry funded Dedicated Card and Payment Crime Unit arrested over 100 fraudsters during the year, including criminals involved in Covid-19 scams.

We also share intelligence on emerging threats with law enforcement and across the banking and finance industry. UK Finance's Information and Intelligence Unit helped protect over 2.1 million compromised card numbers in 2020. The industry is also working closely with the government on measures to strengthen the fight against fraud and economic crime, including through the Economic Crime Strategic Board jointly chaired by the home secretary and chancellor.

However, the banking and finance sector is reaching the limits of what it can do alone. In recent years, we have seen the biggest drivers of fraud moving outside the banking industry to other sectors, a trend that has only been exacerbated by the Covid-19 pandemic. Criminals are increasingly evading banks' advanced security systems through social engineering scams that target people directly, tricking them into giving away their money and personal or financial information. These scams are becoming ever more sophisticated, using technology and the internet to make their approaches more convincing. This has translated into a continued rise in authorised push payment fraud, where people are convinced to transfer funds to a criminal themselves.

The banking industry introduced a voluntary Code in May 2019 which has meant more victims of these scams are reimbursed. UK Finance's latest figures show £147 million of losses were reimbursed under the Code in 2020, accounting for 47 per cent of losses in these cases. We recognise, however, that the voluntary Code is not always working as intended, with a lack of consistency in customer outcomes and a lack of clarity for signatories in how to implement it. We support calls for new legislation for Authorised Push Payment fraud to provide clarity to firms, deliver more consistent outcomes for customers and ensure that protections under the Code apply across the financial services industry.

However, we also need to focus on stopping this fraud happening in the first place. Given the rising threat posed by these scams, we believe more must be done by all sectors to address vulnerabilities in their systems that are being exploited by criminals to target people. This includes everything from phishing emails to data breaches, spoof phone calls and texts as well as scams advertised on social media and search engines. UK Finance is working closely with the telecommunications sector to mitigate this threat, including a successful initiative with the mobile phone industry to block scam text messages and work with telecoms regulator Ofcom to prevent criminals spoofing the phone numbers of trusted organisations.

But we need big tech companies to do more to clamp down on the fraud being perpetrated on their platforms. Nearly every scam now has an online element, whether it is investment scams promoted on search engines or money mules recruited via social media. It's clear the current legal and regulatory framework needs to be updated to keep pace with the rapid growth in these online scams. Currently, the tech giants are not properly held accountable for fraudulent content promoted on their platforms. In some cases, these firms are even being paid by the criminals to place scam adverts on their platforms. It cannot be right that online platforms are profiting from these scams, while the rest of society is left to pay the price.

UK Finance is therefore calling on the government to include fraud and economic crime within the upcoming Online Safety Bill. This would require large tech firms to address vulnerabilities in their systems and stop consumers from being ruthlessly exploited by criminals. We want to see online platforms take action at every stage to stop these scams, ensuring better protection for consumers, and less money for the criminal gangs responsible.

Katy Worobec
Managing Director, Economic Crime
UK Finance

FOREWORD

LexisNexis® Risk Solutions is delighted to sponsor this year's Fraud the Facts report. We see great value in combining this essential information on fraud losses and case volumes across the industry with our own Cybercrime Report[1], which focuses on fraud attacks detected during near real-time consumer interactions online.

Our Cybercrime Report, based on the analysis of 26.5 billion transactions monitored by the LexisNexis® Digital Identity Network®[2] from July to December 2020, corroborates many of the findings reported in Fraud the Facts and provides further insights around key trends to watch out for.

Sadly, the pandemic environment has provided rich pickings for fraudsters, in the form of new-to-digital consumers, heightened vulnerabilities and anxieties, as well as new channels to exploit.

Within the Digital Identity Network, we've seen transaction volumes across financial services grow by 29 per cent globally and 15 per cent in the UK (always considered a frontrunner in its online banking maturity curve). We've also seen growth in online banking registrations across web and mobile during the first UK lockdown period.

Interestingly, corresponding attack rates are down overall, year-on-year, indicating that fraudsters are turning their attention to other, potentially easier targets, such as new lines of credit and Covid-19 stimulus packages, that are not recorded in the Digital Identity Network.

In addition, the UK online banking profile within the Digital Identity Network is more mobile than ever, with more than 85 per cent of transactions originating from a mobile device. From a fraud perspective, banking via a mobile app is the safest way to transact – with a much lower attack rate than either mobile or desktop browser transactions. The main point of vulnerability remains the device registration; compromise here leads to the keys to the kingdom.

This broad picture, however, belies the fact that organised, networked fraud plays a pernicious role in the UK financial services landscape, both at a macro level in the form of organised mule rings, and at a micro level, of individual fraudsters using scams to dupe unsuspecting customers.

Many of the attack patterns witnessed in the Digital Identity Network over the course of 2020 correlate with the organised and ruthless nature of attacks noted by UK Finance.

Although overall attacks declined, we did see a growth in automated bot attacks; the method of choice for testing stolen identity credentials. Perhaps 2020 was a year that created opportunity for fraudsters to automate their jobs at scale, and the impact of these identity testing attacks may yet be felt across the industry.

At the macro level, we analysed a network of fraudsters operating across ten financial services institutions in the UK. This network comprised thousands of transactions, from 7,800 devices, with at least £12 million exposed to fraud across the network.

Likewise, we witnessed several examples of fraudsters preying on Covid-19-related support or vulnerability. One such example saw fraudsters upgrading consumer bank accounts to business ones in order to qualify for the government's Bounce Back Loan scheme. They then applied for multiple loans across multiple UK banks. Several of these applications were linked to known mule activity.

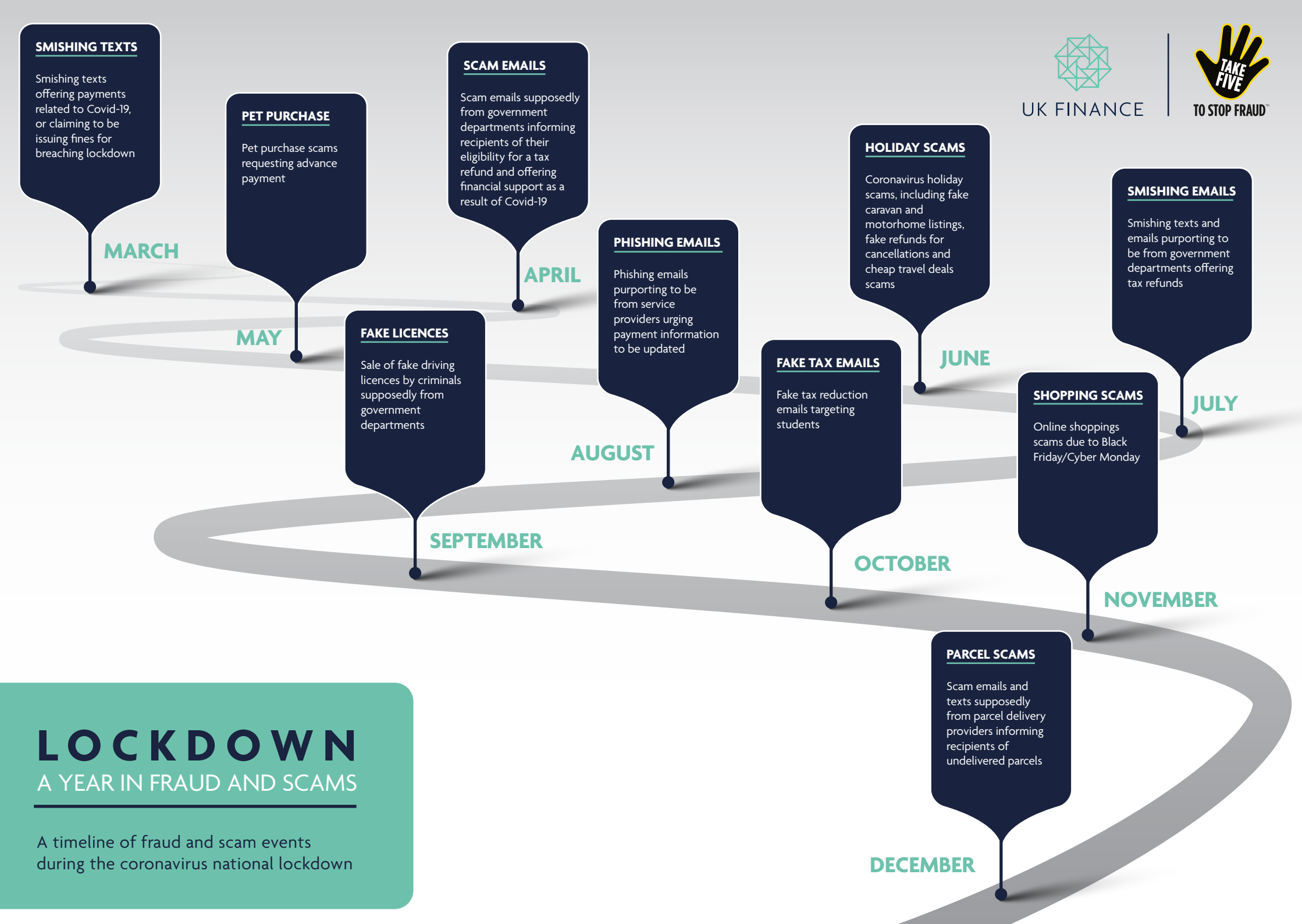
These two examples further highlight the importance of the industry working together to share intelligence to mitigate this complex and networked pattern of fraud. LexisNexis Risk Solutions has a UK banking consortium that allows its members to share information related to confirmed fraud events, with confidence and context. This capability was used to help detect activity related to those fraudulent Bounce Back Loan applications.

Protecting the full spectrum of banking customers is key, but particular effort should be focused on those new-to-digital users and vulnerable customers who may be more susceptible to fraud attack. We found that the youngest age group of under 25s experienced the highest rate of fraud attack, followed by the oldest age group of over 75s. This places the onus on education, awareness and protection of all groups of society, whether they are just starting their online banking journey, or using it for the first time.

Rebekah Moody
Director, Fraud & Identity,
LexisNexis® Risk Solutions

1. Download The LexisNexis® Risk Solutions Cybercrime Report, July to December 2020 at risk.lexisnexis.com/GlobalCybercrimeTrends

2. LexisNexis® Digital Identity Network® is the world's largest network of digital identities, bringing together global crowdsourced intelligence from over 40 billion transactions every year, including web and mobile identification, true location and behavioural analysis, identity and link analysis and bot and malware threat intelligence. It provides a 360-degree view of customers by merging offline and online data in near real time to establish true digital identities.



LOCKDOWN

A YEAR IN FRAUD AND SCAMS

A timeline of fraud and scam events during the coronavirus national lockdown

TRENDS AND STATISTICS

2020 overview

Unauthorised financial fraud losses across payment cards, remote banking and cheques totalled £783.8 million in 2020, a decrease of five per cent compared to 2019.

Banks and card companies prevented £1.6 billion in unauthorised fraud in 2020. This represents incidents that were detected and prevented by firms and is equivalent to £6.73 in every £10 of attempted fraud being stopped.

In addition to this, UK Finance members reported 149,946 incidents of Authorised Push Payment (APP) scams in 2020 with gross losses of £479 million.

Behind the changing fraud figures

Throughout 2020 there has been significant growth in the use by criminals of social engineering to trick consumers out of their money. This is a tactic by which criminals use psychological manipulation to trick people into making security mistakes or giving away sensitive information. Social engineering attacks happen in one or more steps.

In particular, the Covid-19 pandemic has seen criminals ruthlessly adapt and evolve their methods to take advantage of the increase in remote working and people spending more time online and being more contactable by email. While online fraud and scams have been increasing for some years – as consumers have turned to online services for many aspects of their day-to-day lives – criminals have used social engineering to prey on people's fears and uncertainties about the pandemic and defraud them.

Highlighting this, impersonation scams saw the biggest increase of any scam type, almost doubling in 2020 compared to 2019. For example, criminals have turned to mass scam texts, phone calls and emails impersonating trusted organisations such as the NHS, the police or the government to trick people into giving away their personal and financial details. One such scam, purporting to be from the NHS, invited people to provide their personal and financial details in order to 'receive the vaccine'.

Throughout 2020, criminals also continued to impersonate other trusted organisations such as banks, utility companies, e-commerce firms, delivery companies and broadband providers in a bid to defraud consumers.

Increasingly criminals have been preying on people's financial insecurities during the pandemic through investment scams promising high returns. Previously criminals typically used cold calling to target their victims. However, intelligence indicates that they are now using sophisticated techniques to commit this form of fraud, including abusing Search Engine Optimisation and creating fake

comparison websites to drive customers to cloned scam websites. Customers will often be instructed to complete online forms to register their interest, before receiving a call from someone impersonating a genuine investment firm or broker. Criminals will also sometimes send out professional-looking fake documentation to make the scam appear more convincing, or provide access to online portals that claim to allow the victim to monitor how their investment is performing.

Criminals are also using social media and digital messaging services to promote bogus investment opportunities, including in forex trading and cryptocurrency – the latter fuelled by the success of and demand for currencies such as Bitcoin and Ethereum.

The pandemic has also helped to drive up cases of romance fraud, as social distancing restrictions led to a significant increase in online dating and provided an opportunity for criminals to take advantage of this.

In fact, nearly every scam now exploits some sort of online vulnerability, whether it be investment scams promoted on search engines, fake goods listed on auction sites or romance fraudsters abusing online dating sites.

The latest fraud figures show there has been a significant rise in internet and mobile banking fraud in 2020, driven in part at least by growing use of these channels. Figures from 2019 show that 81 per cent of the adult population used at least one form of remote banking and this is only likely to have increased due to the impact of the pandemic. Internet banking losses have increased, with fraudsters increasingly targeting victims directly through phishing emails and using social engineering techniques to trick them into giving away their passcodes and log in details.

There has also been an increase in criminals recruiting people to become money mules – this is where people are paid to receive money into their account before transferring it to another account, with the funds being stolen or illegally obtained. Money mule recruiters have been posting fake adverts on jobs websites and social media to target those looking for work, particularly young people who have been hardest hit by the economic impact of the pandemic.

However, the Covid-19 pandemic has led to a fall in contactless card and cheque fraud in 2020 as the lockdown restrictions reduced opportunities for criminals to commit these types of scams.

The industry response

The banking and finance industry is working hard to protect customers from fraud and scams, while partnering with law enforcement to catch and prosecute the criminal gangs responsible. It is responding to this threat by:

- Investing in advanced security systems to protect customers from fraud, including real-time transaction analysis. The industry prevented £1.6 billion of unauthorised fraud in 2020, equivalent to £6.73 in every £10 of attempted unauthorised fraud being stopped.
- Working with the government and law enforcement to establish clear strategic priorities, with improved accountability and coordination through the Economic Crime Strategic Board, jointly chaired by the Home Secretary and the Chancellor. The **Economic Crime Plan** sets out how to harness the combined capabilities of the public and private sectors better to make the UK a leader in the global fight against economic crime.
- Coordinating a joint response to economic crime and sharing intelligence on emerging threats with law enforcement, government departments and regulators through the **National Economic Crime Centre**. This has a shared objective of driving down serious organised economic crime, protecting the public and safeguarding the prosperity and reputation of the UK as a financial centre.
- UK Finance is working with the government, law enforcement and regulators to develop a more advanced Fraud Action Plan.
- Sharing intelligence across the banking and finance industry on emerging threats, data breaches and compromised card details via UK Finance's Information and Intelligence Unit (I&I Unit). In 2020, 2.1 million compromised card numbers were received through our law enforcement strategic partners and disseminated via the I&I unit to enable card issuers to take the necessary precautions to protect customers.
- The industry is working with law enforcement to stop fraud through initiatives such as the **Banking Protocol**, a scheme which allows bank branch staff to alert the police when they think a customer is being scammed. This initiative stopped £45.3 million of fraud and led to 200 arrests in 2020. This means it has now prevented a total of £142 million of fraud and resulted in 843 arrests since it was rolled out in 2016. The scheme is currently being expanded to telephone and online banking, which has been particularly important for vulnerable customers who have been unable to visit their local branch as a result of the coronavirus lockdown restrictions.
- Fully funding a specialist police unit, the Dedicated Card and Payment Crime Unit (DCPCU), which tackles the organised criminal groups responsible for financial fraud and scams. Throughout 2020 the unit **prevented** an estimated £20 million of fraud, arrested 122 suspected fraudsters, and carried out enforcement activity against criminals exploiting Covid-19 to target their victims. The unit has also worked with social media platforms to take down over 700 accounts linked to fraudulent activity in 2020, of which over 250 were money mule recruiters.

- Working with text message providers and law enforcement to **block** scam text messages including those exploiting the Covid-19 crisis. 1087 unauthorised sender IDs are currently being blocked to prevent them being used to send scam text messages mimicking trusted organisations, including more than 70 related to Covid-19.
- Working with the regulator **Ofcom** to crack down on number spoofing, including through the development of a 'do not originate' list. Ofcom has said this work has led to significant successes in preventing criminals from spoofing the phone numbers of trusted organisations. For example, when HMRC added numbers to this list they reported reducing "to zero the number of phone scams spoofing genuine inbound HMRC numbers".
- Working with Cifas on the **Don't Be Fooled** campaign, which aims to inform students and young people about the risks of giving out their bank details and deter them from becoming money mules.
- Working with Pay.UK to implement the Mule Insights Tactical Solution (MITS), a technology that helps to track suspicious payments and identify money mule accounts.
- Working with Pay.UK to implement Confirmation of Payee, an account name-checking service that helps prevent authorised push payment scams. Since 30 June 2020 the measure has been fully implemented by the UK's six largest banking groups, and has since expanded to cover more than a dozen payment providers. More than a million Confirmation of Payee requests are made every day covering over 90% of Faster Payments volumes. More providers are expected to sign up in 2021.
- Helping customers stay safe from fraud and spot the signs of a scam through the **Take Five to Stop Fraud** campaign. 30 major banks and buildings societies have signed up to the **Take Five Charter**, bringing the industry together to give people simple and consistent fraud awareness advice.

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 payments online, a second level of security is required, such as a one-time passcode sent via text message or biometrics. The FCA has set a deadline for the implementation of the SCA rules by 14 September 2021.

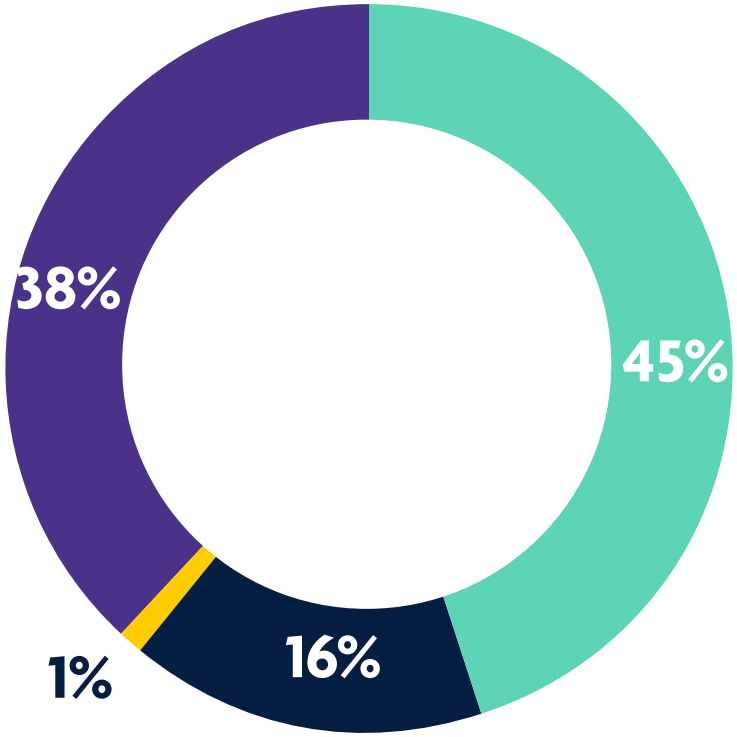
To combat telephone banking fraud, some banks are using technology which allows them to identify the different sound tone that every phone has and the environment that they are in. If someone is calling from an environment which is not their usual one, this can be picked up and investigated further to 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 2020 financial fraud losses by type

TOTAL 2020 FRAUD LOSS	£1.26bn



- Payment Card
- Remote Banking
- Cheque
- Authorised Push Payment

CARD FRAUD

Unauthorised debit, credit and other payment card fraud

VALUE	£574.2m	- 7%

VOLUME	2,835,622	+3%

Fraud losses on UK-issued cards totalled £574.2 million in 2020, a seven per cent fall from £620.6 million in 2019. Data for total spending on all debit and credit cards are not yet available but the report will be updated to reflect these figures once UK Finance has received them.

A total of £983 million in card fraud was stopped by banks and card companies in 2020, a fall of two per cent compared to 2019. This is equivalent to £6.31 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 (SCA) 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 FCA has set a deadline of 14 September for the full implementation of SCA.
- 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.
- Funding a specialist police unit, the Dedicated Card and Payment Crime Unit (DCPCU), which tackles the organised criminal gangs responsible for financial fraud and scams. Throughout 2020 the unit **prevented** an estimated £20 million of fraud and arrested 122 suspected fraudsters.

Fraud Type	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	% Change 19/20
Remote Purchase (CNP)	£221.0	£247.3	£301.0	£331.5	£398.4	£432.3	£408.4	£506.4	£470.2	£452.6	-4%
Of which e-commerce	£139.6	£140.2	£190.1	£219.1	£261.5	£310.3	£310.4	£394.2	£360.5	£376.5	4%
Counterfeit	£36.1	£42.3	£43.3	£47.8	£45.7	£36.9	£24.2	£16.3	£12.8	£8.7	-32%
Lost & Stolen	£50.1	£55.4	£58.9	£59.7	£74.1	£96.3	£92.9	£95.1	£94.8	£78.9	-17%
Card ID Theft	£22.5	£32.6	£36.7	£30.0	£38.2	£40.0	£29.8	£47.3	£37.7	£29.7	-21%
Card non-receipt	£11.3	£12.8	£10.4	£10.1	£11.7	£12.5	£10.2	£6.3	£5.2	£4.4	-15%
Total	**£341.0**	**£390.4**	**£450.2**	**£479.0**	**£568.1**	**£618.1**	**£565.4**	**£671.4**	**£620.6**	**£574.2**	**-7%**
UK	£260.9	£288.4	£328.2	£328.7	£379.7	£417.9	£407.5	£496.6	£449.9	£414.5	-8%
Fraud Abroad	£80.0	£102.0	£122.0	£150.3	£188.4	£200.1	£158.0	£174.8	£170.7	£159.7	-6%

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

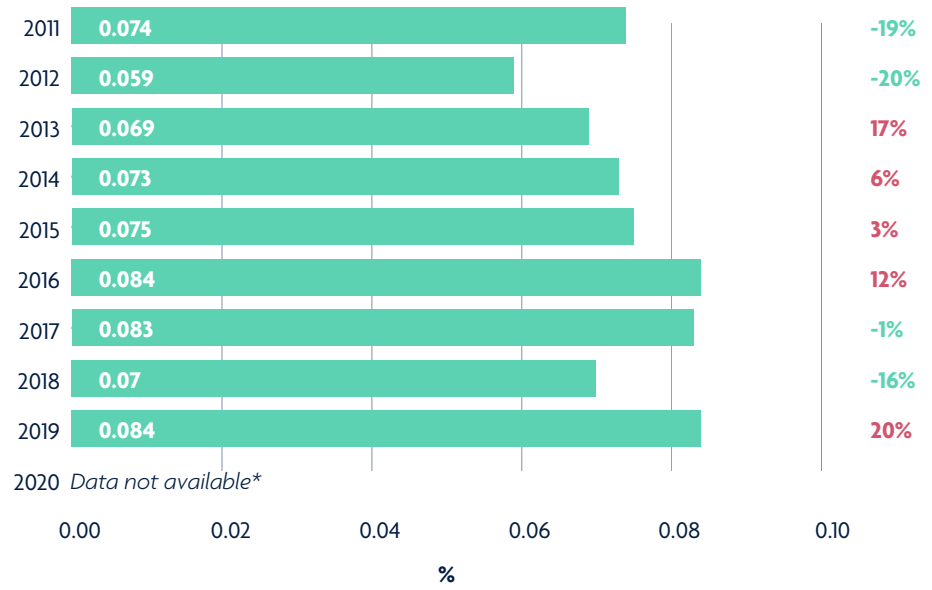
UK Finance also publishes the number of fraud incidents to convey more fully the dynamics of the fraud environment in the UK. Whilst losses have been decreasing, the number of confirmed cases has increased during 2020, rising by four per cent to 2,835,622 cases. This demonstrates that cases are being spotted and stopped by card issuers more quickly, with a lower average loss per case (£381 in 2010 down to £203 in 2020).

There was a rise in the number of cases involving remote purchase fraud in 2020, which has driven the overall rise in fraud volumes. However, cases of fraud on lost and stolen cards have fallen significantly due to the restrictions in movement as a result of the pandemic.

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.

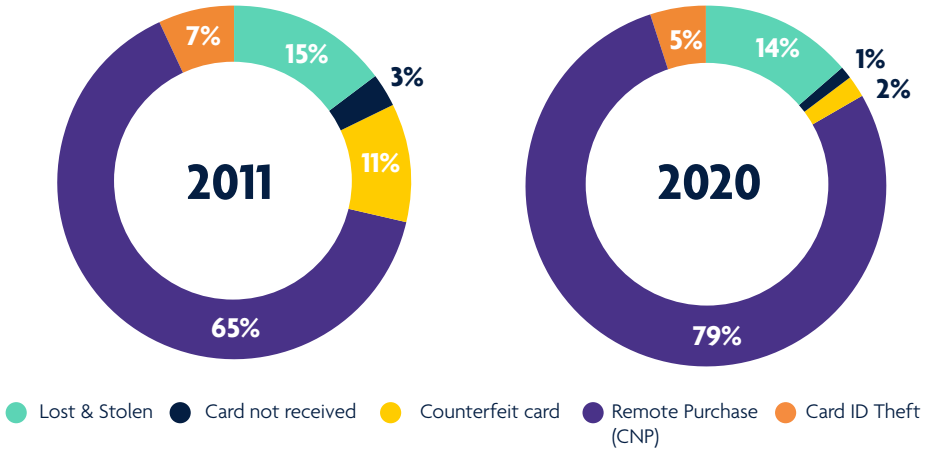
Card Fraud Type on UK-issued credit and debit cards	2016	2017	2018	2019	2020	% Change 19/20
Remote Purchase (CNP)	1,437,832	1,398,153	2,050,275	2,157,418	2,417,866	12%
Counterfeit (skimmed/cloned)	108,597	85,025	58,636	65,907	52,782	-20%
Fraud on lost or stolen cards	231,164	350,279	434,991	460,142	321,994	-30%
Card ID theft	31,756	29,156	63,791	54,165	34,545	-36%
Card non-receipt	11,377	10,903	10,046	7,907	8,435	7%
Total	**1,820,726**	**1,873,516**	**2,617,739**	**2,745,539**	**2,835,622**	**3%**

Fraud to turnover ratio 2011 – 2020 (£m)



**Data for total spending on all debit and credit cards in 2020 are not yet available but the report will be updated to reflect these figures once UK Finance has received them.*

Card fraud losses 2020 split by type (as a percentage of total losses)



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

VALUE	£452.6m	-4%

VOLUME	2,417,866	+12%

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 fell to £452.6 million in 2020, a decrease of four per cent when compared to 2019. Online fraud against UK retailers totalled an estimated £262.3 million in 2020, a nine per cent increase on the previous year. Mail or telephone order (MOTO) fraud against retailers based in the UK totalled £63.7 million, a 28 per cent decrease compared to 2019.

Overall card fraud losses are down on last year, but levels remain high as fraudsters exploit the significant rise in online card spending during the pandemic. However, the 12 per cent increase in the number of cases of remote purchase fraud when compared with a four per cent decrease in gross losses suggests that card issuers are identifying and stopping individual incidents more quickly.

Intelligence suggests remote purchase fraud continues to result largely from criminals using card details obtained through data theft, such as third-party data breaches and via phishing emails and scam text messages. This includes scams exploiting the coronavirus pandemic by impersonating trusted organisations such as the government and NHS, for example asking people to enter their card details to book a Covid-19 vaccine.

Criminals are also using social media profiles to advertise the 'sale' of discounted goods to consumers. When a customer buys the product, the criminal uses stolen card details to purchase the same item from a legitimate source and keeps the payment from the customer.

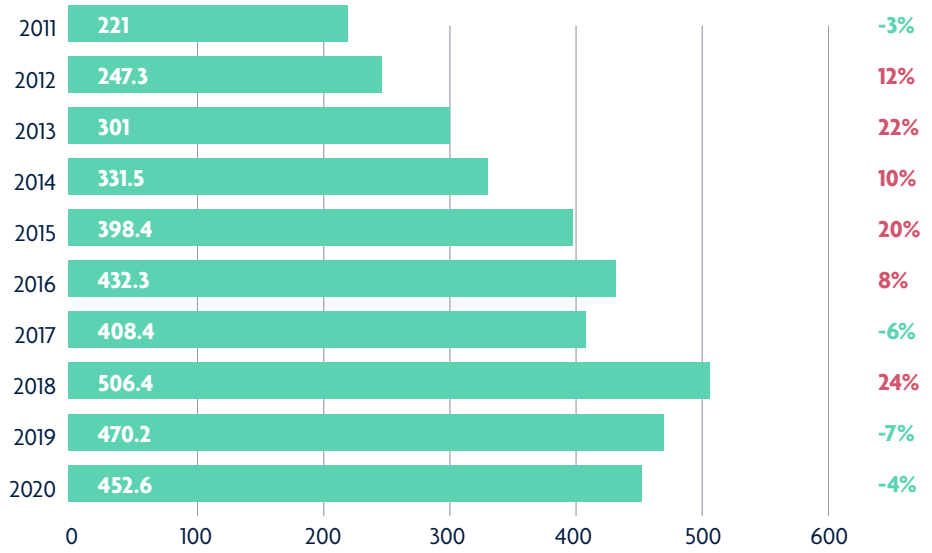
Criminals continue to deploy "digital skimmers" to steal card data from customers when they shop online. In a typical digital skimming attack, criminals will add malicious code to the online retailer's website which steals sensitive information including card details at the check-out stage. This information is then sent to a domain controlled by criminals, who use it to commit remote purchase fraud. These attacks continue to highlight the importance of online retailers maintaining robust security measures, including by ensuring payment platforms are regularly updated with the latest software.

The industry is working on the phased implementation of Strong Customer Authentication, new rules aimed at reducing fraud by verifying a customer's identity when they make certain higher value online purchases. The Financial Conduct Authority (FCA) has currently set a **deadline** for these rules to be fully implemented in the UK by 14 September 2021.

However, in an attempt to circumvent these additional protections, criminals are increasingly using social engineering techniques to trick customers into divulging their One Time Passcodes (OTPs) so they can authenticate fraudulent online card transactions. In some cases, customers are also being tricked by criminals into making online card transactions themselves.

OTPs should be treated in the same way as your PIN in that they should never be shared with anyone, including your bank. Before entering your OTP make sure you check it accurately describes the transaction/purchase you're about to make. Your bank will never contact you asking for your full account details, PIN or your passcodes. If you receive a code you weren't expecting, contact your bank or the police immediately on a phone number you know to be genuine, such as the one listed on the back of your debit or credit card.

Remote purchase (CNP) fraud losses on UK-issued cards 2011 – 2020 (£m)



How to stay safe from remote purchase fraud:

- Be suspicious of any 'too good to be true' offers or prices.
- Use the secure payment method recommended by reputable online retailers and auction sites.
- Where possible, use a credit card when making purchases over £100 and up to £30,000 as you receive protection under Section 75 of the Credit Consumer Act.
- Read online reviews to check websites and sellers are genuine, and ask to see high value items in person or via video link, as well as getting copies of the relevant documentation to ensure the seller owns the item.
- Purchase items made by a major brand from the list of authorised sellers listed on their official website.
- Always access the website you're purchasing from by typing it into your web browser and be wary of clicking on links in unsolicited emails.
- Always ensure you click 'log out' or 'sign out' of websites.
- The introduction of Lucy's Law makes it illegal for you to purchase pets sold by a third-party seller. If you're looking for a pet, buy it directly from a breeder or consider adopting from a rescue centre instead.

Counterfeit card fraud

VALUE	£8.7m	-32%

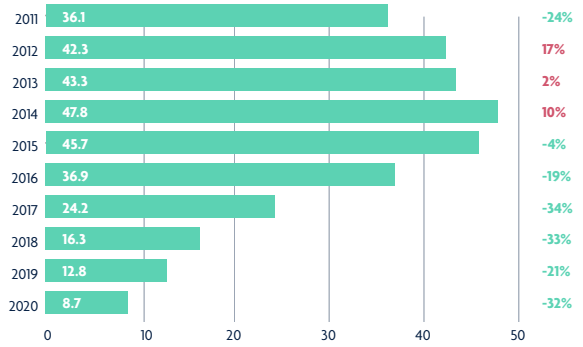
VOLUME	52,782	-20%

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

Counterfeit card losses totalled £8.7 million in 2020, a fall of nearly a third (32 per cent) compared to 2019 and 95 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 which are 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 & PIN has not been adopted to use counterfeit cards for financial advantage.

Counterfeit card fraud losses on UK-issued cards 2011 – 2020 (£m)



How to stay safe from counterfeit card fraud:

- Always protect your PIN by covering the keypad with your free hand ,purse or wallet.
- If you spot anything suspicious when using an ATM, 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, contact your bank or card company immediately.

Lost and stolen card fraud

VALUE	£78.9m	-17%

VOLUME	321,994	-30%

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 bank branch.

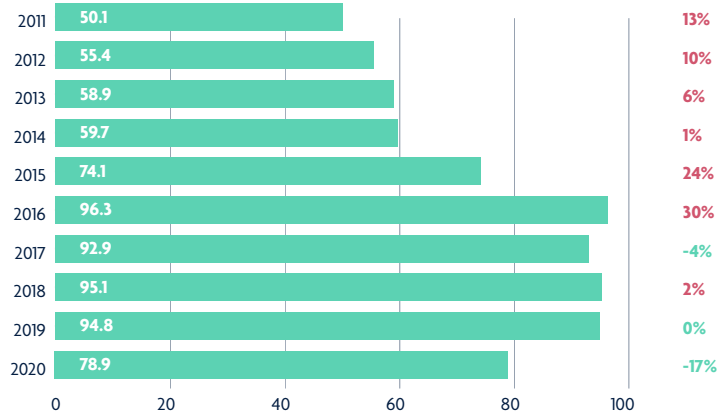
Losses due to lost and stolen fraud dropped by 17 per cent in 2020, falling to £78.9 million compared to £94.8 million in 2019. The number of incidents also decreased sharply, falling by 30 per cent over the same period. The majority of this type of fraud occurs using cards obtained through low-tech methods such as distraction thefts and entrapment devices at ATMs. 2020 saw the first annual decrease in contactless losses since we began collecting data. The fall in contactless card fraud was in part due to the reduced opportunities for fraudsters to commit these types of scams because of lockdown restrictions during the pandemic.

The contactless payment limit was increased from £30 to £45 in in April 2020, following consultation between the retail sector and the finance and payments industry, to support consumers who choose to pay using contactless at this time.

The Financial Conduct Authority and Treasury have announced the contactless payment limit will now be increased further to £100. UK Finance will work closely with the payments sector and retailers ahead of increasing the limit later this year.

The industry continues to deploy a range of fraud prevention and detection tools to protect consumers from contactless card fraud. These tools remain highly effective in the fight against this type of fraud. Each card 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. (For more information on contactless see page 32).

Lost and stolen card fraud losses on UK-issued cards 2011 – 2020 (£m)



How to stay safe from lost and stolen fraud:

- Always report 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, contact your bank or card company immediately.

Card ID theft

VALUE	£29.7m	-21%

VOLUME	34,545	-36%

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 21 per cent in 2020, to £29.7 million, with the number of cases decreasing by 36 per cent to 34,545. 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.

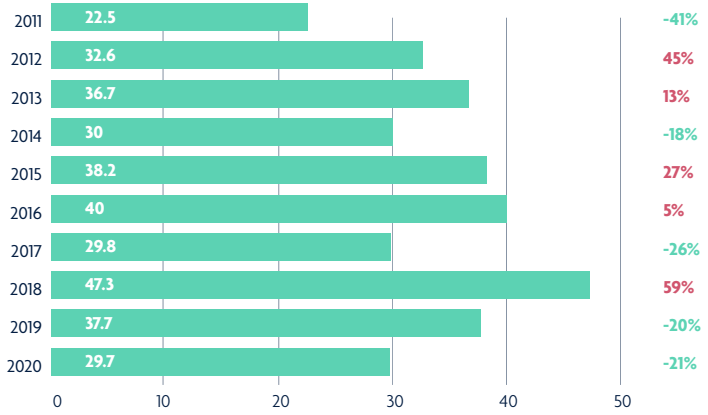
Application fraud – £15.1 million (-13%)

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 - £14.6 million (-28%)

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 2011 – 2020 (£m)



How to stay safe from card ID fraud:

- Use a redirection service when moving to a new home such as the one provided by the Royal Mail as well as informing your bank, card company and other organisations of your new address.
- Destroy unwanted documents including bills, bank statements or post that's in your name, preferably by using a shedder.
- Request copies of your personal credit report from a credit reference agency on a regular basis to check for any entries you don't recognise.
- Provide as little personal information about yourself on social media as possible and only accept invitations from people you know.
- You can apply to be on the **Cifas Protective Registration Service** for a fee which places a flag next to your name and personal details in their secure National Fraud Database. Companies and organisations who have signed up as members of the database can see you're at risk and take extra steps to protect you, preventing criminals from using your details to apply for products or services.
- Be careful if other people have access to your post. Contact Royal Mail if you think your post is being stolen.
- Cancel any lost or stolen credit or debit cards immediately.
- Keep your personal information secure when using your card over the phone, on the internet, or in shops by ensuring that others can't overhear you or see your information.
- If your passport, driving licence, cards or other personal information have been lost or stolen, immediately contact the organisation that issued it.

Card not received fraud

VALUE	£4.4m	-15%

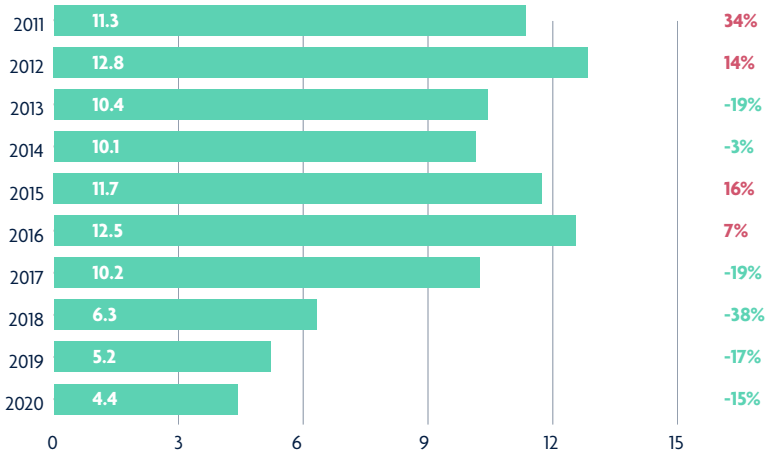
VOLUME	8,435	+7%

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 15 per cent in 2020 to £4.4 million. However, the volume of cases rose by seven per cent, indicating that measures put in place to detect such frauds early on are having a beneficial effect as the average case value has decreased.

Criminals typically target properties with communal letterboxes, such as flats, 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 2011-2020 (£m)



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 company immediately if you move home. Use the Royal Mail redirection service to redirect your post to your new address for at least a year.
- Be extra vigilant if you live in a property where other people may have access to your mail, such as a block of flats. In some cases, your bank or card company can 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	£ 48.9m	-24%

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 24 per cent in 2020 to £48.9 million. Given the extended periods in 2020 when the majority of shops were closed due to Covid-19 restrictions, this has unsurprisingly had a beneficial effect in reducing cases of such fraud.

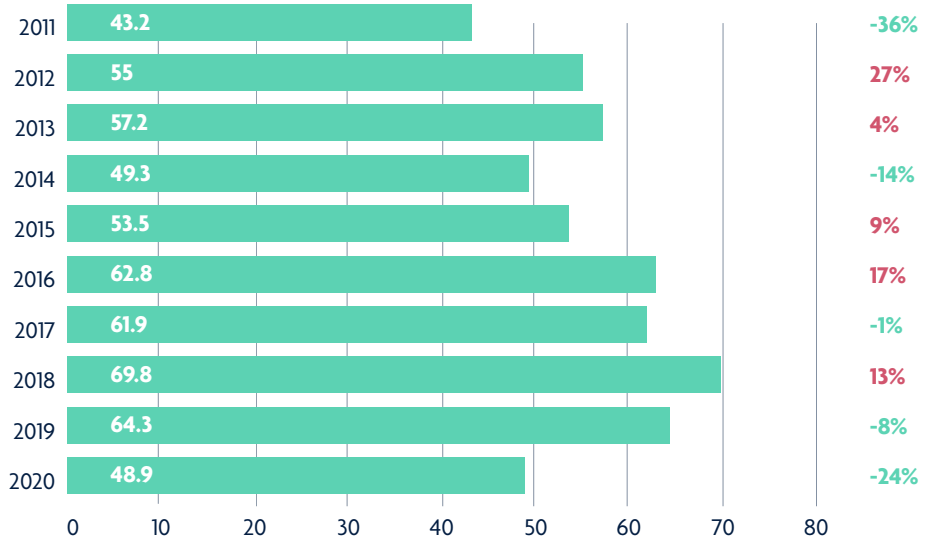
The majority of this fraud is undertaken using low-tech techniques, with fraudsters finding ways of stealing the card, and often the PIN, to carry out fraudulent transactions in shops. This includes criminals using methods such as ATM card entrapment and distraction thefts, combined with shoulder surfing 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 £16 million of losses during 2020, compared to spending of £9.46 billion over the same period.

This is equivalent to 1.8p in every £100 spent using contactless technology, a reduction in the total recorded in 2019 (2.7p). Contactless fraud on payment cards and devices represents just 2.9 per cent of overall card fraud losses, while 55 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) 2011-2020 (£m)



COMMON MISCONCEPTIONS ABOUT CONTACTLESS CARD PAYMENTS AND FRAUD

1. **Criminals can steal my details from my contactless card**
   You must be extremely close to someone for them to be able to read your card. Even then, they would only get the card number and expiry date which is the same information you see by simply looking at the front of any card.

   There's no way anyone can access to the important details such as the security code on the back of the card.

   As the vast majority of online retailers require additional details like these to make a purchase, there is very little chance of a fraudster being able to make online transactions.

2. **A fraudster could take money from my card just by bumping into me in the street or on public transport**
   There has never been any verified report of this ever happening in the UK. It's not possible to simply 'steal' cash from a contactless card. All money must go through the card system.

   You must have a retail account to get any money from a card payment. There are thorough security checks before these can be set up and new accounts are continuously monitored for any suspicious activity. Every card payment is fully traceable, right through to the recipient account.

   Finally, a contactless card must be used in a specific way to work. That means it can only be a few centimetres away from the card reader and not near any metal objects, like keys and mobile phones, or any other contactless card.

3. **If I lose my card all my money can be taken through contactless transactions**
   Every card has an in-built security check which means from time-to-time you have to enter your PIN to verify that you are the genuine cardholder. You can also only spend a maximum of £45 in any single contactless card transaction.

   However, if you lose your card, or think it might have been stolen, then you should contact your bank straight away.

   You are fully protected against fraud, so you get all of your money back and will never be left out of pocket. If you notice any suspicious activity on your account, contact your bank immediately.

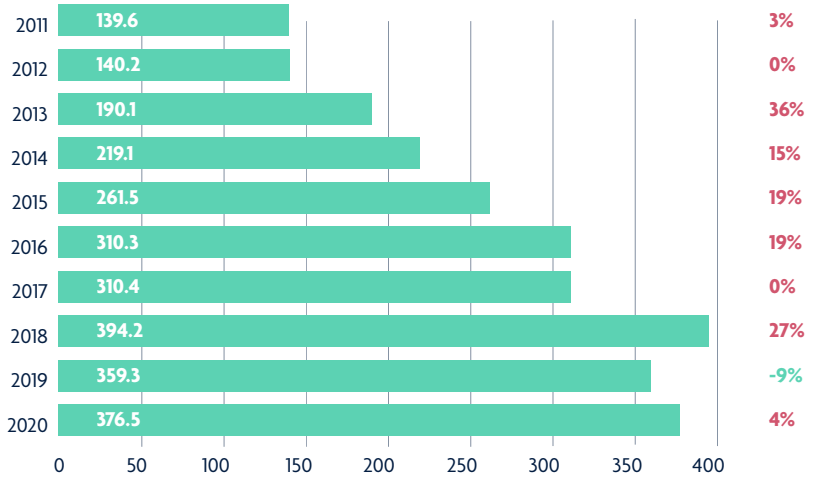
Internet/e-commerce fraud

VALUE	£376.5m	+4%

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 £376.5 million of e-commerce fraud took place on cards in 2020, accounting for 66 per cent of all card fraud and 83 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. 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.

Internet/e-commerce fraud losses on UK-issued cards 2011-2020 (£m)



Card fraud at UK cash machines

VALUE	£28.1m	-6%

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 – the latter is likely to have been less common in 2020 as bars and many shops were closed for long periods of time.

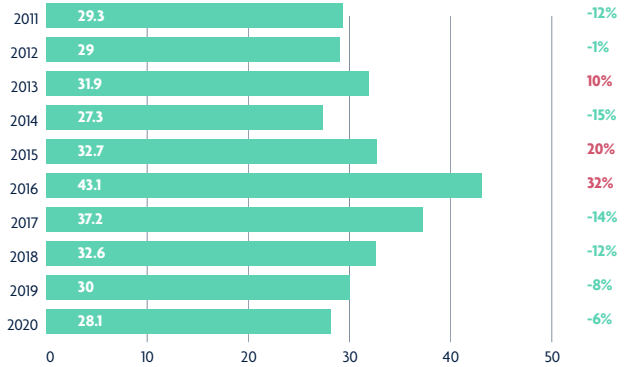
Fraudsters also target cash machines to compromise or steal cards or card details in three main ways:

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 2011-2020 (£m)



Card fraud abroad

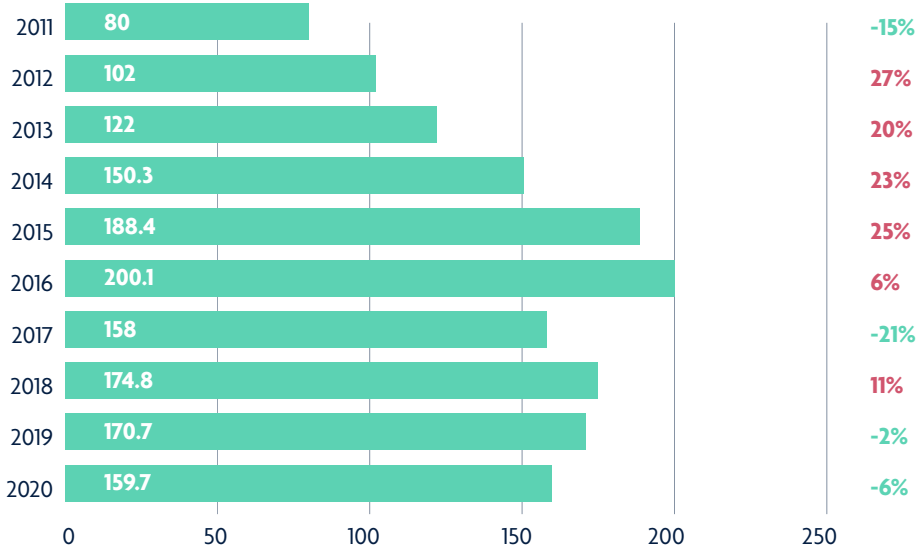
VALUE	£159.7m	-6%

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.

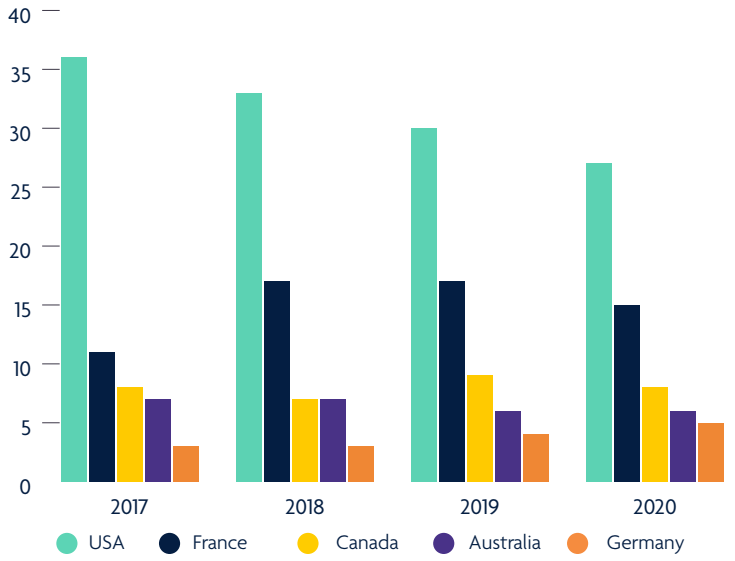
International fraud losses for 2020 were £159.7 million, compared with losses at their peak in 2008 of £230.1 million, a decrease of 31 per cent.

Fraud committed abroad on UK-issued cards 2010-2020 (£m)



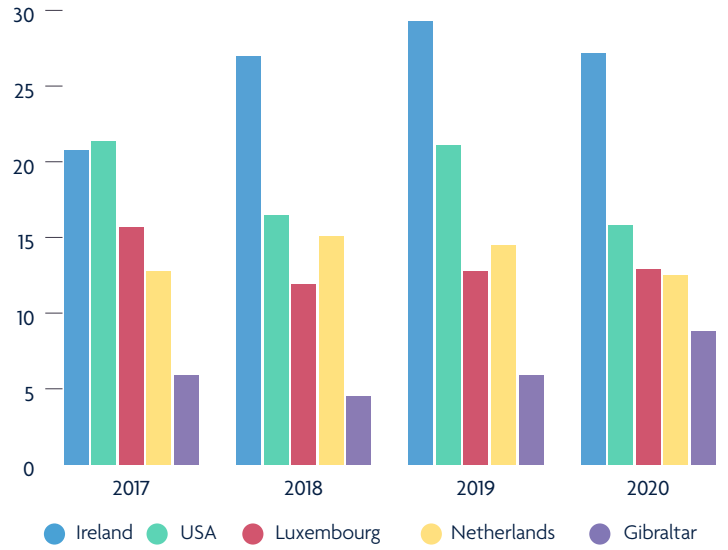
Top five countries for fraud on foreign-issued cards occurring in the UK 2017-2020

Losses are shown as a percentage of total fraud at UK-acquired merchants on foreign-issued cards.



Top five countries where fraud on UK-issued cards occurs 2017-2020

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



CHEQUE FRAUD

Cheque fraud

VALUE	£12.3m	-77%

VOLUME	1,247	-56%

Cheque fraud losses fell to £12.3 million in 2020, down from £53.6 million in 2019. Meanwhile the volume of fraudulent cheques decreased by 56 per cent. The fall in cheque fraud is likely to have been driven by the continued fall in the use of cheques, which in turn has been exacerbated by the impact of lockdown restrictions.

The banking industry continues to carry out internal checks to tackle cheque fraud, including advanced security features on business cheques to identify fraudulent ones as they go through the clearing process. It is also working closely with law enforcement to target the organised criminal gangs operating cheque fraud. This includes a major successful investigation by the industry-funded Dedicated Card and Payment Crime Unit into a UK-wide cheque fraud network that had scammed businesses and charities out of £750,000.

A total of £238.5 million of cheque fraud was prevented in 2020, down 57 per cent on 2019. This reflects the fact that the levels of fraud attack reduced in 2020, following the spike in 2019 which was due to vulnerabilities identified in the move from the paper-based cheque paying in system to the image-based clearing system, which banks have now addressed.

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

Counterfeit cheque fraud - £7.2 million (-83%)
Counterfeit cheques are printed on non-bank paper to look exactly like genuine cheques and are drawn by a fraudster on genuine accounts.

Fraudulently altered cheques - £1.8 million (-70%)
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.

Forged cheque fraud - £3.3 million (-48%)
A forged 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.

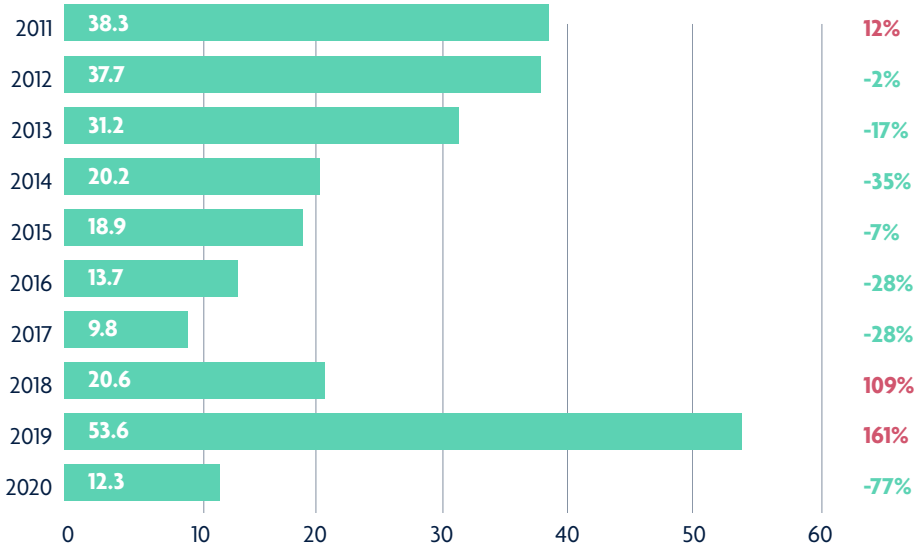
Prevented Cheque Fraud 2015 - 2020

Cheque	2015	2016	2017	2018	2019	2020	19/20 % Change
Prevented Value	£392.8m	£196.2m	£212.3m	£218.2m	£550.8m	£238.5m	-57%

Annual case volumes cheque fraud 2015-2020

Cheque	2015	2016	2017	2018	2019	2020	19/20 % Change
Cheque fraud cases	5,746	3,388	1,745	2,020	2,852	1,247	-56%

Cheque Fraud losses 2011-2020 (£m)



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 and report any missing cheques to your bank immediately.
- Check your statements regularly and if you spot any payments you don't recognise, contact your bank or building society immediately

UNAUTHORISED REMOTE BANKING FRAUD

Unauthorised remote banking fraud

VALUE	£197.3m	+31%

VOLUME	73,640	+68%

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 £197.3 million in 2020, 31 per cent higher than seen in 2019. The number of cases of remote banking fraud increased by 68 per cent to 73,640. 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. Furthermore the pandemic has pushed growing numbers of people towards online and mobile banking due to restrictions on movement and an increase in people working from home – situations that fraudsters have made every attempt to take advantage of.

A total of £393.8 million of attempted remote banking fraud was stopped by bank security systems during 2020. This is equivalent to £2 in every £3 of fraud attempted being prevented. In addition, 15 per cent (£30.2 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 2013-2020

Remote banking values	2013	2014	2015	2016	2017	2018	2019	2020	19/20 % Change
Internet banking	£58.8m	£81.4m	£133.5m	£101.8m	£121.2m	£123.0m	£111.8m	£159.7m	43%
Telephone banking	£13.1m	£16.8m	£32.3m	£29.6m	£28.4m	£22.0m	£23.6m	£16.1m	-32%
Mobile banking	N/A	N/A	£2.8m	£5.7m	£6.5m	£7.9m	£15.2m	£21.6m	41%
TOTAL	**£71.7m**	**£71.9m**	**£98.2m**	**£137.0m**	**£156.1m**	**£152.9m**	**£150.7m**	**£197.3m**	**31%**

Annual case volumes Remote Banking fraud 2013-2020

Remote banking cases	2013	2014	2015	2016	2017	2018	2019	2020	19/20 % Change
Internet banking	13,799	16,041	19,691	20,088	21,745	20,904	25,849	55,995	117%
Telephone banking	5,596	5,578	11,380	10,495	9,577	7,937	11,199	7,490	-33%
Mobile banking	N/A	N/A	2,235	2,809	3,424	2,956	6,872	10,155	48%
Total	**19,395**	**21,819**	**33,306**	**33,392**	**34,746**	**31,797**	**43,920**	**73,640**	**68%**

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.
- Expanding the Banking Protocol scheme, a scheme which allows bank branch staff to alert the police when they think a customer is being scammed, to telephone and online banking, in particular to help vulnerable customers who have been unable to visit their local branch as a result of the coronavirus lockdown restrictions.
- 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	£159.7m	+43%

VOLUME	55,995	+117%

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

Typically, criminals employ a range of social engineering techniques to trick victims into giving away their personal and financial information, such as their internet banking One Time Passcodes and log in details. This includes using a high volume of impersonation scam calls, emails or text messages exploiting the pandemic by impersonating trusted organisations such as HMRC, Internet Service Providers and e-commerce companies. The stolen details are then used to access a customer's online account and to make an unauthorised transaction.

The fact that many people have been working from home, spending longer online and doing more internet shopping, may have made may them more susceptible to these scams. Intelligence suggests that customers of all age groups are falling victim to these scams, but particularly across younger age groups.

Meanwhile, over two thirds of UK adults (72 per cent) used online banking in 2019 and this proportion is expected to have increased further in 2020 as a result of the pandemic. As the use of internet and online banking increases, so do attempts by criminals to steal money through these channels.

Fraudsters are also abusing remote access software applications to gain control of their victim's online banking facilities.

The criminals will typically claim to be providing support from an IT service or internet service provider and convince the customer to download and install remote access applications to their laptop PC or devices.

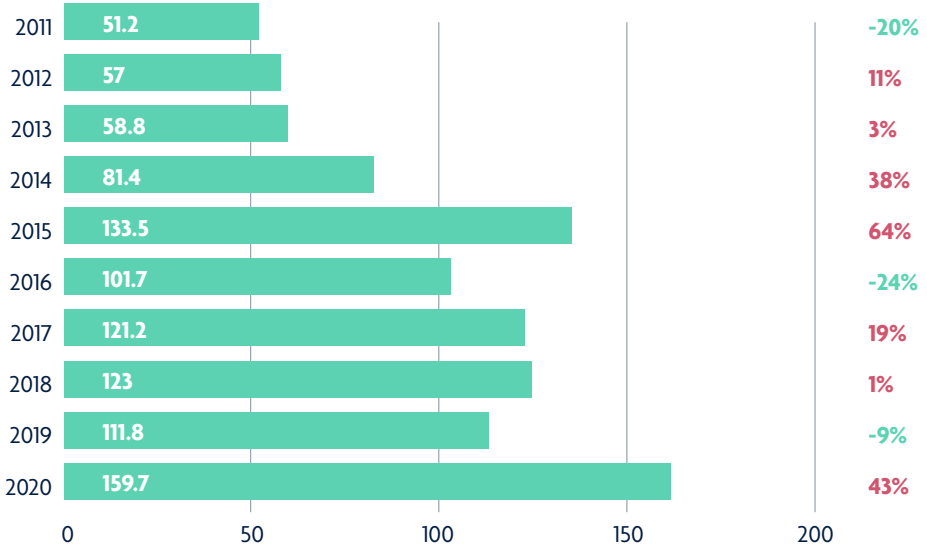
There has been a significant rise in the use of phishing websites to obtain customers' online banking credentials. Over 25,000 bank-branded phishing websites were identified and taken down in 2020, four times higher than the previous year.

The banking industry has been working hard during the pandemic to support customers who are not used to banking online, including through digital lessons and guides.

A total of £326.2 million of attempted internet banking fraud was stopped by bank security systems during 2020. This is equivalent to £6.71 in every £10 of fraud attempted being prevented. In addition, 16 per cent (£25.3 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 2011-2020 (£m)



Annual case volumes for internet banking fraud 2012-2020

	2012	2013	2014	2015	2016	2017	2018	2019	2020	19/20 % Change
Internet Banking Fraud	16,355	13,799	16,041	19,691	20,088	21,745	20,904	25,849	55,995	117%

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, full password or passcodes. Only give out your personal or financial details to use a service to which you have given your consent, that you trust and by which you are expecting to be contacted.
- 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	£16.1m	-32%

VOLUME	7,490	-33%

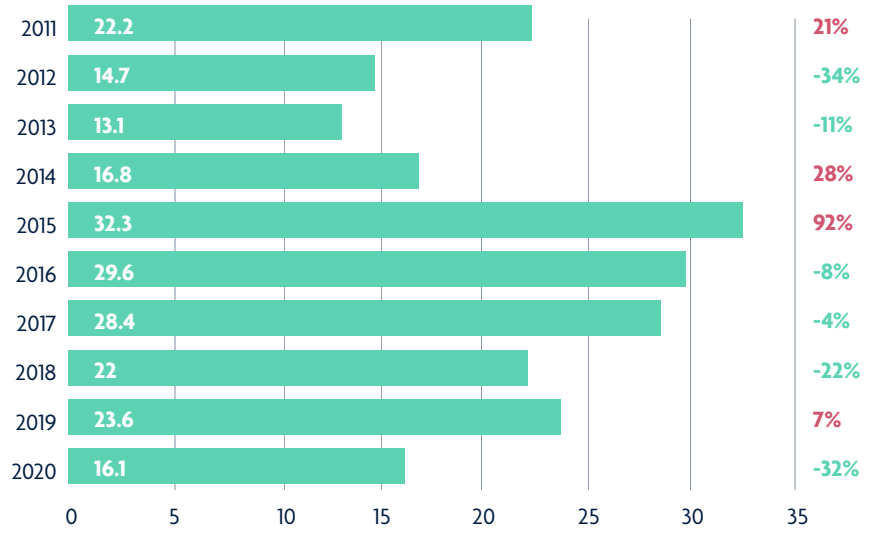
This type of fraud occurs when a criminal gains access to the victim's telephone banking account and makes an unauthorised transfer of money away from it.

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 £58 million of attempted telephone banking fraud was stopped by bank security systems during 2020. This is equivalent to £7.82 in every £10 of fraud attempted being prevented. In addition, 12 per cent (£2 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 2011-2020 (£m)



Annual case volumes for telephone banking fraud 2012-2020

	2012	2013	2014	2015	2016	2017	2018	2019	2020	19/20 % Change
Telephone Banking Fraud	7,095	5,596	5,778	11,380	10,495	9,577	7,937	11,199	7,490	-33%

How to stay safe from telephone banking fraud:

- Never disclose security details, such as your full banking password or passcode. A genuine financial provider or organisation will never ask you for these in an email, on the phone or in writing.
- Never give remote access to any of your devices while on the phone as fraudsters may then be able to log in to your online banking.
- Always question uninvited approaches for your personal or financial information 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, your mother's maiden name, or even your direct debits and transactions), it doesn't mean they are genuine.

Mobile banking fraud

VALUE	£21.6m	+41%

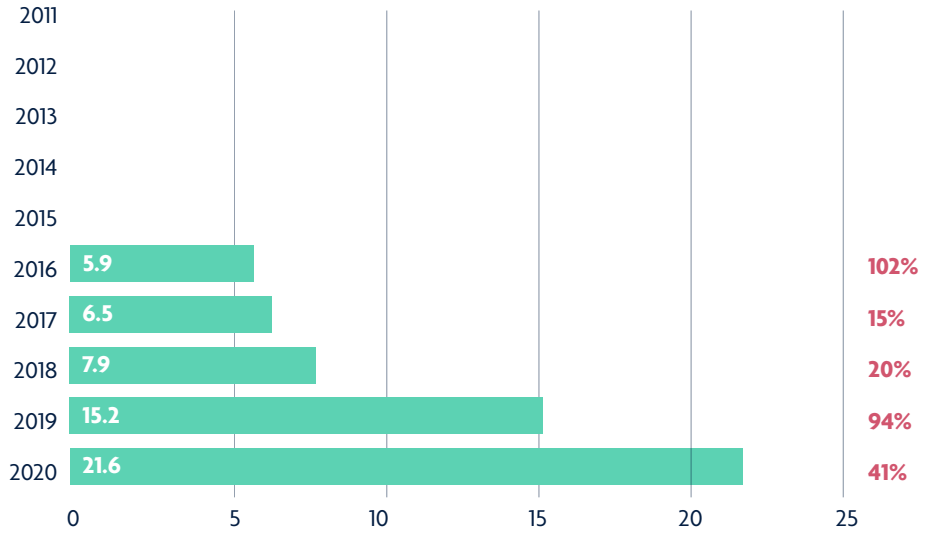
VOLUME	10,155	+48%

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. In 2019, at least 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, and this is likely to continue rising as people become more familiar with and comfortable with mobile banking, and the functionality offered through mobile banking improves.

A total of £9.6 million of attempted mobile banking fraud was stopped by bank security systems during 2020. This is equivalent to £3.09 in every £10 of fraud attempted being prevented. In addition, 13 per cent (£2.9 million) of the losses across the mobile banking channel were recovered after the incident.

Mobile banking fraud losses 2016-2020 (£m)



Annual case volumes for mobile banking fraud 2015-2020

	2012	2013	2014	2015	2016	2017	2018	2019	2020	19/20 % Change
Mobile Banking Fraud	N/A	N/A	N/A	2,235	2,809	3,424	2,956	6,872	10,155	48%

How to stay safe from mobile banking fraud:

- Don't be tricked into giving a fraudster access to your personal or financial information. Never automatically click on links in unexpected emails or texts and always question uninvited approaches.
- Be wary of text messages that encourage you urgently to visit a website or phone 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	£479m	+5%

VOLUME	149,946	+22%

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 data now includes the scam type, payment type and payment channel.

- Since May 2019, following work between the industry, consumer groups and the regulator, a voluntary code on authorised push payment (APP) scams has been in place that provides protections for customers of signatory payment service providers (PSPs). It delivers a commitment from all signatory firms to reimburse victims of authorised push payment fraud as long as the customer has met the standards expected of them under the code. To fund compensation for eligible victims of APP scams where the customer, sending and recipient banks have met the standards expected of them expected under the Code, a number of launch signatories of the Code established an interim funding arrangement to provide reimbursement until a long-term solution is in place. To fund this compensation, a number of launch signatories of the Code established an interim funding arrangement to provide reimbursement until a long-term solution is in place. The seven launch signatories who have provided interim funding in these situations under the Code have **agreed** to continue the funding to 30 June 2021.
- Nine PSPs, representing 19 consumer brands and over 85 per cent of authorised push payments, have signed up to the Code so far. A list of signatories can be found **here**.

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 £479 million in 2020. This was split between personal (£387.8 million) and non-personal or business (£91.3 million).

In total there were 149,946 cases. Of this total, 143,259 cases were on personal accounts and 6,687 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 and, as highlighted earlier in the report, the use of social engineering tactics to defraud people has only increased during the pandemic. Typically, such deception and impersonation scams involve 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 worked with Pay.UK to implement new technology that helps track suspicious payments and identify money mule accounts.

While the total number of APP fraud cases seen in 2020 rose by 22 per cent as criminals increasingly looked to take advantage of the pandemic to defraud people, total APP fraud losses rose by just five per cent in 2020 compared to 2019, as measures introduced by banks helped to prevent many larger-scale fraud attempts.

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 2019 - 2020

		PERSONAL			NON PERSONAL			TOTAL		
		2019	2020	% Change	2019	2020	% Change	2019	2020	% Change
Volume	Cases	114,731	143,259	25%	7,706	6,687	-13%	122,437	149,946	22%
	Payments	174,798	233,868	34%	10,651	11,933	12%	185,449	245,801	33%
Value	Value	£317.1m	£387.8m	22%	£138.7m	£91.3m	-34%	£455.8m	£479.0m	5%
	Reimbursed	£82.2m	£170.8m	108%	£33.8m	£36m	7%	£116.0m	£206.9m	78%

APP Voluntary Code statistics

The authorised push payment (APP) scams voluntary code was introduced on 28 May 2019, following work between the industry, consumer groups and the regulator. 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.

This is the second year that UK Finance is publishing statistics relating to the cases assessed using the voluntary code and the compensation provided to customers. It shows that 139,104 cases have been assessed and closed since the code was introduced, with a total value of £311.8 million. Our latest figures show that £147.0 million of losses were reimbursed to victims under the APP voluntary Code in 2020, accounting for 47 per cent of losses in these cases. This is up from 41 per cent of losses being reimbursed in cases assessed under the Code in 2019, and more than double the 19 per cent of APP losses that were reimbursed before the Code was introduced. A total of £188.3 million has been reimbursed to thousands of customers since the Code was introduced in May 2019.

Reimbursement levels in 2020 were higher for more sophisticated scams in which criminals impersonate other organisations to target their victims. For police and bank impersonation scams, 53 per cent of all losses were refunded to the victim; the second highest of all eight scam types. Other impersonation scams had the highest reimbursement rate of all eight scam types, with 57 per cent of all losses refunded to victims.

Reimbursement rates were also higher for APP cases involving higher, life-changing sums of money. 48 per cent of losses were reimbursed in those cases involving values of £10,000 or more, compared to 32 per cent of losses reimbursed for cases involving values of less than £1,000.

UK Finance and its members have worked to ensure all cases in which customers are reimbursed, including cases where the bank was able to trace and return the original stolen funds, are now included within these figures. This may account for some of the increase in the proportion of losses being reimbursed in cases assessed under the Code compared to previous fraud updates.

Only those cases assessed using the voluntary code by signatory PSPs

All cases reported below are also 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	102,645	30,505	5,954	**139,104**
	Payments	128,606	64,836	21,843	**215,285**
Value	Value	£29.0m	£100.2m	£182.6m	**£311.8m**
	Reimbursed	£9.5m	£44.0m	£87.3m	**£147.0m***

**This includes £6.3 million of reimbursement for cases where a repatriation of funds has occurred from the beneficiary account after the case has been reported and the funds are subsequently returned to the victim. It is not possible to attribute the totals to specific scam types but they are included to reflect the true value reimbursed to victims for those cases which have been assessed using the code.*

The finance industry is tackling authorised push payment scams by:

- Introducing the industry-wide APP scams voluntary code, which helps to improve protections and reimburse many victims of these scams.
- Developing a secure mechanism to enable firms to share information about confirmed APP frauds with a view to enhancing the industry's ability to freeze and repatriate funds.
- 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 and Don't Be Fooled campaigns.
- Delivering the Banking Protocol – a ground-breaking rapid response scheme through which branch staff can alert police to suspected frauds taking place. The system is now operational in every police force area and has prevented £142 million in fraud and led to 843 arrests since launching in 2016. The scheme is currently being expanded to telephone and online banking, which has been particularly important for vulnerable customers who have been unable to visit their local branch as a result of the coronavirus lockdown restrictions.
- 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 2020 the Unit prevented an estimated £20 million of fraud, arrested 122 fraudsters, and secured 54 convictions. The unit also worked with social media platforms to take down 700 accounts linked to fraudulent activity, of which over 250 were money mule recruiters.
- Working with Pay.UK to implement the Mules Insights Tactical Solution (MITS), a new technology that helps to track suspicious payments and identify money mule accounts.
- Working with Pay.UK on the ongoing implementation of Confirmation of Payee, an account name checking service that helps to prevent authorised push payment scams, used when a payment is being made.
- 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 provide further insight into APP scams. These data cover:

- Eight scam types: Malicious Payee (Purchase scam, Investment scam, Romance scam and Advance fee scam) and Malicious Redirection (Invoice & Mandate scam, CEO Fraud, Impersonation: Police/Bank Staff and Impersonation: Other).
- Six payment types: Faster Payment, CHAPS, BACS (Payment), BACS (Standing Order), Intra-bank ("on-us") and International.
- Four payment channels: Branch, Internet Banking, Telephone Banking and Mobile Banking.

The data in the following sections provide a breakdown of the overall APP scam data detailed in the earlier section and are 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.

APP SCAM TYPES

Malicious payee

Purchase scams

VALUE	£57.1m	-3%	VOLUME	78,720	+7%

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 2020, with the 78,720 cases accounting for 52 per cent of the total number of APP scam cases. A total of £57.1 million was lost to purchase scams in 2020, with the vast majority of losses being from personal accounts. Payment service providers were subsequently able to return £16.3 million of the losses.

Typically, purchase scams involve lower-value payments, with the smaller average case value meaning that they accounted for only 12 per cent of the total value of APP scams.

All Purchase scam cases reported 2019 – 2020

		PERSONAL			NON PERSONAL			TOTAL		
		2019	2020	% Change	2019	2020	% Change	2019	2020	% Change
Volume	Cases	71,574	76,595	7%	1,762	2,125	21%	73,336	78,720	7%
	Payments	90,942	99,827	10%	2,178	2,775	27%	93,120	102,602	10%
Value	Value	£51.1m	£49.5m	-3%	£7.9m	£7.7m	-3%	£59.0m	£57.1m	-3%
	Reimbursed	£8.9m	£14.1m	60%	£0.8m	£2.2m	166%	£9.7m	£16.3m	69%

Only those cases assessed using the voluntary code by signatory PSPs

All cases reported below are also 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	58,752	6,445	342	65,539
	Payments	73,156	11,386	1,008	85,550
Value	Value	£13.8m	£18.4m	£7.5m	£39.7m
	Reimbursed	£3.1m	£4.9m	£2.9m	£10.9m

For those cases which were applicable for assessment using the voluntary code in 2020, 28 per cent of all losses were repatriated to the victim; the smallest proportion across all eight of the scam types. However, this is an increase from the ten per cent being reimbursed in the six months before the code was introduced (Jan to June 2019).

90 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 for a purchase scam.
- Where possible, use a credit card when making purchases over £100 and up to £30,000 as you receive protection under Section 75 of the Credit Consumer Act.
- Always access the website you're purchasing from by typing it into your web browser and be wary of clicking on links in unsolicited emails.
- Always ensure you click 'log out' or 'sign out' of websites.
- The introduction of Lucy's Law makes it illegal for you to purchase pets sold by a third-party seller. If you're looking for a pet, buy it directly from a breeder or consider adopting from a rescue centre instead.

Investment scams

VALUE	£135.1 m	+42%

VOLUME	8,958	+32%

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.

A total of £135.1 million was lost to investment scams in 2020, with payment services providers subsequently able to return £49 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 28 per cent of the total value.

All Investment scam cases reported 2019 - 2020

		PERSONAL			NON PERSONAL			TOTAL		
		2019	2020	% Change	2019	2020	% Change	2019	2020	% Change
Volume	Cases	6,679	8,722	31%	110	236	115%	6,789	8,958	32%
	Payments	13,962	22,713	63%	261	540	107%	14,223	23,253	63%
Value	Value	£89.5m	£125.4m	40%	£5.9m	£9.7m	65%	£95.4m	£135.1m	42%
	Reimbursed	£11.7m	£47m	301%	£0.6m	£2m	255%	£12.3m	£49m	299%

Only those cases assessed using the voluntary code by signatory PSPs

All cases reported below are also 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**	2,922	2,016	1,759	**6,697**
	Payments	4,905	5,694	6,017	**16,616**
Value	**Value**	£1.1m	£7.5m	£73.9m	**£82.6m**
	Reimbursed	£0.3m	£1.9m	£30.7m	**£32.9m**

For only those cases which were applicable for assessment using the voluntary code, 40 per cent of all losses were repatriated to the victim in 2020; in the six months before the code was introduced (Jan to June 2019) just seven per cent was reimbursed.

How to stay safe from investment scams:

- Be cautious of approaches presenting you with exclusive investment opportunities. It could be a scam if you're being pressurised to act quickly.
- Most cryptocurrencies aren't regulated by the FCA which means they're not protected by the UK's Financial Services Compensation Scheme. It's important that you do your research and proceed with extreme caution before making any investments
- Check the **Financial Conduct Authority's register** for regulated firms, individuals and bodies. You can check their website is genuine by checking their web address. It should always begin with fca.org.uk or register.fca.org.uk. Ensure you only use the contact details listed on the Register to confirm you're dealing with the genuine firm before parting with your money and information.
- You can check if an investment or pension opportunity you've been offered could potentially be a scam by taking the **FCA's ScamSmart test**.
- Report scam ads appearing in paid-for space online by visiting the **Advertising Standard Authority's website** where you can complete their quick reporting form.

Romance scams

VALUE	£21.2m	+17%

VOLUME	2,984	+38%

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 £21.2 million was lost to romance scams in 2020. 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 2020 and four per cent of the total value. Payment service providers were only able to return £8.1 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 2019 - 2020

		PERSONAL			NON PERSONAL			TOTAL		
		2019	2020	% Change	2019	2020	% Change	2019	2020	% Change
Volume	Cases	2,137	2,947	38%	26	37	42%	2,163	2,984	38%
	Payments	10,956	14,745	35%	61	127	108%	11,017	14,872	35%
Value	Value	£18.0m	£20.6m	15%	£0.1m	£0.5m	388%	£18.1m	£21.2m	17%
	Reimbursed	£2.3m	£8m	244%	£0.0m	£0.1m	314%	£2.4m	£8.1m	244%

Only those cases assessed using the voluntary code by signatory PSPs

All cases reported below are also 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**	817	775	279	**1,871**
	Payments	2,163	5,050	3,211	**10,424**
Value	**Value**	£0.3m	£3.0m	£8.9m	**£12.1m**
	Reimbursed	£0.1m	£0.9m	£3.6m	**£4.6m**

For only those cases which were applicable for assessment using the voluntary code, 38 per cent of all losses were returned to the victim in 2020. In the six months before the code was introduced (Jan to June 2019) only six per cent was reimbursed.

How to stay safe from romance scams:

- Avoid sending money to someone you've never met in person, particularly if you have only recently met online.
- Research the person you're talking to as profile photos may not be genuine. You can do this by uploading a picture of the person you're talking to into search engines to check that profile photos are not associated with another name. Performing a **reverse image search** can find photos that have been taken from somewhere, or someone, else.
- Be alert to spelling and grammar mistakes and inconsistencies in stories.
- Stay on the dating site or on the messaging service until you're confident the person is who they say they are and ensure meetings in person take place in public.
- Always consider the possibility of a scam.
- Only accept friend requests from people you know and trust.
- Speak to your family or friends to get advice

Advance fee scams

VALUE	£23m	+34%

VOLUME	14,128	+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 materialise. These scams often begin with an email or a letter sent by the criminal to the victim.

Advance fee scams were the fourth most common form of APP scam in 2020, accounting for nine per cent of the total number of cases. A total of £23.0 million was lost to advance fee scams last year, meaning by value these scams accounted for nearly five per cent of all APP scams.

All advance fee scam cases reported 2019 - 2020

		PERSONAL			NON PERSONAL			TOTAL		
		2019	2020	% Change	2019	2020	% Change	2019	2020	% Change
Volume	Cases	10,508	13,769	31%	203	359	77%	10,711	14,128	32%
	Payments	16,828	23,500	40%	276	526	91%	17,104	24,026	40%
Value	Value	£16.0m	£21.9m	38%	£1.3m	£1.1m	-13%	£17.2m	£23.0m	34%
	Reimbursed	£2.1m	£7.7m	260%	£0.1m	£0.3m	131%	£2.3m	£8m	252%

Only those cases assessed using the voluntary code by signatory PSPs

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

		Less than £1k	£1k - £10k	More than £10k	Total
Volume	**Cases**	9,052	2,169	237	**11,458**
	Payments	12,797	5,136	1,470	**19,403**
Value	**Value**	£3.0m	£5.6m	£7.4m	**£16.0m**
	Reimbursed	£0.8m	£1.6m	£2.5m	**£4.9m**

For only those cases which were applicable for assessment using the voluntary code, 30 per cent of all losses were returned to the victim in 2020 . In the six months before the code was introduced (Jan to June 2019) only eight per cent was reimbursed.

How to stay safe from advance fee scams:

- Question claims that you're due money for goods or services that you haven't ordered or are unaware of, especially if you have to pay any fees upfront.
- It's extremely unlikely that you've won a lottery or competition that you haven't entered, and which requires an upfront fee.
- Check the email address of recruiters or employers to ensure they're genuine and be vigilant of those platforms that businesses would be unlikely to use e.g. Yahoo, Hotmail or Gmail.
- Confirm organisations you're being contacted by are registered on **Companies House** and use the details provided to contact recruitment companies and other organisations directly. You can check their website is genuine by checking their web address.
- Be suspicious of fake profiles on social media platforms e,g. LinkedIn offering jobs that don't exist.
- Make sure you use a reputable recruitment company who are a member of a trade association such as the **REC**, **APSCo** and **TEAM**. You can check this by looking for the association logos on the company's website or by visiting the trade association's website directly and searching by member.
- If you're concerned about a job scam you can report it to a trade association and to **SAFERjobs** using their online reporting tool.
- Contact your bank straight away if you think you may have fallen for an advance fee scam.

Malicious Redirection

Invoice and mandate scams

VALUE	£81.9m	-28%

VOLUME	4,955	-42%

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 sixth most common type of APP scam in 2020, however they accounted for 17 per cent of all APP losses, totalling £81.9 million. The majority of losses by value, some £52.5 million, were from non-personal or business accounts, where the average payment was £18,871. This reflects the fact that businesses make higher-value payments more regularly.

All invoice and mandate scam cases reported 2019 - 2020

		PERSONAL			NON PERSONAL			TOTAL		
		2019	2020	% Change	2019	2020	% Change	2019	2020	% Change
Volume	Cases	4,732	2,967	-37%	3,840	1,988	-48%	8,572	4,955	-42%
	Payments	6,387	4,313	-32%	5,081	2,783	-45%	11,468	7,096	-38%
Value	Value	£31.7m	£29.4m	-7%	£82.4m	£52.5m	-36%	£114.1m	£81.9m	-28%
	Reimbursed	£12.8m	£15.3m	20%	£19.5m	£22m	13%	£32.3m	£37.3m	16%

Only those cases assessed using the voluntary code by signatory PSPs

All cases reported below are also 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**	1,224	1,755	506	**3,485**
	Payments	1,458	2,222	1,022	**4,702**
Value	**Value**	£0.5m	£6.0m	£20.9m	**£27.4m**
	Reimbursed	£0.3m	£3.1m	£11.1m	**£14.5m**

For only those cases which were applicable for assessment using the voluntary code, 53 per cent of all losses were returned to the victim. In the six months before the code was introduced (Jan to June 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 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 for an invoice or mandate scam.

CEO fraud

VALUE	£10.4m	-41%

VOLUME	837	+24%

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 2020, accounting for less than one per cent of total cases. A total of £10.4 million was lost, equivalent to two per cent of the total case value.

All CEO fraud scam cases reported 2019 - 2020

		PERSONAL			NON PERSONAL			TOTAL		
		2019	2020	% Change	2019	2020	% Change	2019	2020	% Change
Volume	Cases	80	440	450%	596	397	-33%	676	837	24%
	Payments	153	519	239%	809	612	-24%	962	1,131	18%
Value	Value	£1.2m	£3.1m	151%	£16.5m	£7.3m	-56%	£17.8m	£10.4m	-41%
	Reimbursed	£0.3m	£1.2m	260%	£3.5m	£2.7m	-24%	£3.9m	£3.9m	1%

Only those cases assessed using the voluntary code by signatory PSPs

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**	27	128	57	**212**
	Payments	38	168	107	**313**
Value	**Value**	£0.0m	£0.6m	£1.5m	**£2.1m**
	Reimbursed	£0.0m	£0.3m	£0.6m	**£0.9m**

For only those cases which were applicable for assessment using the voluntary code, 43 per cent of all losses were refunded to the victim; in the six months before the code was introduced (Jan to June 2019) only 26 per cent was reimbursed.

How to stay safe from CEO fraud:

- Always check unusual payment requests directly, ideally in person or by telephone, to confirm the instruction is genuine. Do not use contact details from an email, text 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, texts 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 for a CEO fraud.

Impersonation: police / bank staff

VALUE	£96.6m	+15%

VOLUME	21,467	+94%

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 14 per cent of all APP scam cases in 2020. £96.6 million was lost due to these scams, which by value was the second highest type of APP scam, accounting for 20 per cent of total losses. Payment service providers were able to return £59.5 million of the losses to customers.

All police/bank impersonation scam cases reported 2019 - 2020

		PERSONAL			NON PERSONAL			TOTAL		
		2019	2020	% Change	2019	2020	% Change	2019	2020	% Change
Volume	Cases	10,835	20,916	93%	253	551	118%	11,088	21,467	94%
	Payments	21,606	39,357	82%	654	2,631	302%	22,260	41,988	89%
Value	Value	£73.5m	£90.2m	23%	£10.7m	£6.4m	-40%	£84.1m	£96.6m	15%
	Reimbursed	£29.6m	£55.4m	88%	£7.8m	£4.1m	-48%	£37.3m	£59.5m	59%

Only those cases assessed using the voluntary code by signatory PSPs

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

		Less than £1k	£1k - £10k	More than £10k	Total
Volume	**Cases**	5,920	11,672	2,035	**19,627**
	Payments	7,595	23,333	6,196	**37,124**
Value	**Value**	£3.4m	£40.9m	£43.8m	**£88.1m**
	Reimbursed	£1.8m	£24.1m	£26.9m	**£52.8m**

For only those cases which were applicable for assessment using the voluntary code, 60 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 (Jan to June 2019) only 26 per cent was reimbursed.

How to stay safe from police/bank impersonation scams:

- Your bank or the police will never ask you to transfer money to a safe account or contact you out of the blue to ask for your PIN, full password or passcode.
- Only give out your personal or financial information to services you have consented to and are expecting to be contacted by.
- Contact your bank or an organisation directly using a known email or phone number.
- Don't give anyone remote access to your computer following a cold call or unsolicited text
- You can forward suspicious emails to **report@phishing.gov.uk** and suspected scam texts to your mobile network provider by forwarding them to 7726. If a scam text claims to be from your bank, then you should also report it to them.

Impersonation: other

VALUE	£53.7m	+7%

VOLUME	17,897	+97%

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 £53.7 million was lost to this type of scam in 2020, with payment service providers subsequently able to return £24.6 million. Impersonation: other scams accounted for 12 per cent of all APP scam cases last year, representing 11 per cent of total losses.

All other impersonation scam cases reported 2019 - 2020

		PERSONAL			NON PERSONAL			TOTAL		
		2019	2020	% Change	2019	2020	% Change	2019	2020	% Change
Volume	Cases	8,186	16,903	106%	916	994	9%	9,102	17,897	97%
	Payments	13,964	28,894	107%	1,331	1,939	46%	15,295	30,833	102%
Value	Value	£36.2m	£47.7m	32%	£14.0m	£6.0m	-57%	£50.2m	£53.7m	7%
	Reimbursed	£14.5m	£21.9m	38%	£1.4m	£2.7m	91%	£15.9m	£24.6m	55%

Only those cases assessed using the voluntary code by signatory PSPs

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**	9,887	5,545	739	**16,171**
	Payments	12,450	11,847	2,812	**27,109**
Value	**Value**	£5.0m	£18.2m	£18.6m	**£41.9m**
	Reimbursed	£1.2m	£7.3m	£9.0m	**£17.5m**

For only those cases which were applicable for assessment using the voluntary code, 42 per cent of all losses were refunded to the victim. In the six months before the code was introduced (Jan to June 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 for an impersonation scam.
- You can forward suspicious emails to **report@phishing.gov.uk** and suspected scam texts to your mobile network provider by forwarding them to 7726. If a scam text claims to be from your bank, then you should also report it to them.
- HMRC will never notify you about tax refunds, penalties or ask for your personal or financial information through emails, texts or phone calls. You can forward suspicious emails claiming to be from HMRC to **phishing@hmrc.gov.uk** and texts to 60599.
- If you're unsure whether it's a scam, check their **guidance on recognising scams**, and for more detail on reporting methods visit **gov.uk**.

Unknown scam type

VALUE £1.9m **VOLUME 14,044**

Within the code there are also some scams where a case classification is not attributed. Some cases assessed under the Code were not attributed to any particular scam type, but are published here for completeness

		Less than £1k	£1k - £10k	More than £10k	Total
Volume	**Cases**	14,044			**14,044**
	Payments	14,044			**14,044**
Value	**Value**	£1.9m			**£1.9m**
	Reimbursed	£1.9m			**£1.9m**

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 96 per cent of cases. While BACS was the least common payment method, representing only 0.4 per cent of casesa and 4 per cent of losses, the high-value nature of transactions using this payment type meant that it accounted for seven per cent of the total value.

Payment type	2019	2020	% Change	2019	2020	% Change
Faster Payment	175,816	235,006	34%	£333.4m	£398.2m	19%
CHAPS	1,340	2,030	51%	£30.0m	£20.5m	-32%
BACS	2,328	867	-63%	£31.5m	£21.0m	-33%
Intra Bank Transfer ("on us")	1,965	1,595	-19%	£3.6m	£6.3m	77%
International	4,000	6,303	58%	£57.4m	£33.0m	-42%
Total	**185,449**	**245,801**	**33%**	**£455.8m**	**£479.0m**	**5%**

Payment Channel

This data shows the channel through which the victim made the authorised push payment. Internet banking was used for 46 per cent of payments, totalling £316.3 million of losses.

Payment type	2019	2020	% Change	2019	2020	% Change
Branch	11,072	8,645	-22%	£49.1m	£45.0m	-8%
Internet Banking	119,224	112,210	-6%	£344.7m	£316.3m	-8%
Telephone Banking	6,001	8,739	46%	£27.5m	£28.5m	4%
Mobile Banking	49,152	116,207	136%	£34.4m	£89.2m	159%
Total	**185,449**	**245,801**	**33%**	**£455.8m**	**£479.0m**	**5%**

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. 36 per cent of cases were decided in less than a week of the case being reported. It should be noted that the decision time does not reflect the amount of time taken for a bank to inform the victim of a liability decision, but how long the case is open on the bank's case management system whilst opportunities for repatriation from the fraudulent beneficiary are explored. Victims will be kept informed throughout the process.

Decision Time	2018	2019	2020
Less than a week	65%	59%	36%
Between week and a month	22%	27%	44%
More than a month	13%	14%	20%

TAKE FIVE TO STOP FRAUD

Take Five is a national campaign that offers straightforward and impartial advice to help everyone protect themselves from preventable financial fraud. This includes email deception and phone-based scams as well as online fraud – particularly where criminals impersonate trusted organisations.

Led by UK Finance, the campaign is 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.

30 major banks and buildings societies have signed up to the **Take Five Charter**, bringing the industry together to give people simple and consistent fraud awareness advice.

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 your 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 you or panic you.
- **PROTECT** – Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud. If you are in Scotland, please report to Police Scotland directly by calling 101 or Advice Direct Scotland on 0808 164 6000.

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

TAKE FIVE TO STOP FRAUD™

This report is intended to provide general information only and is not intended to be comprehensive or to provide legal, regulatory, financial or other advice to any person. Information contained in this report based on public sources has been assumed to be reliable and no representation or undertaking is made or given as to the accuracy, completeness or reliability of this report or the information or views contained in this report. None of UK Finance or any of their respective members, officers, employees or agents shall have any liability to any person arising from or in connection with any use of this report or any information or views contained in this report.
© 2021, UK Finance