UK FINANCE

ANNUAL FRAUD REPORT

THE DEFINITIVE OVERVIEW OF PAYMENT INDUSTRY FRAUD IN 2021

Sponsored by: LexisNexis® RISK SOLUTIONS

UK Finance is the collective voice for the banking and finance industry. Representing around 300 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation.

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

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

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

CONTENTS

OUR FRAUD DATA

UK Finance publishes both the value of fraud losses and the number of cases. The data is reported to us by our members which include financial providers, credit, debit and charge card issuers, and card payment acquirers.

Update on previous fraud figures

Validation checks we undertook on the fraud data supplied to us prior to publication this year uncovered some issues with historic authorised push fraud (APP) figures. We found that some previously published APP figures had been overstated. Updated figures for the first half of 2021 and the whole 2020 are all included within this report.

We have not included any figures for years prior to 2020 as these are now not directly comparable with current data. This is because the manner in which APP losses are identified and reported has changed, following the introduction of UK Finance Best Practice Standards in 2018 and the Contingent Reimbursement Model Code in 2019. In addition, the number of firms reporting APP data to us has increased.

Each incident of fraud does not equal one person being defrauded, but instead refers to the number of cards or accounts defrauded. For example, if a fraud was carried out on two cards, but they both belonged to the same person, this would represent two instances of fraud, not one.

All fraud loss figures, unless otherwise indicated, are reported as gross. This means the figures represent the total value of fraud including any money subsequently recovered by a bank.

Some caveats are required for the tables in the document:

- Prevented values were not collected for all fraud types prior to 2015.
- The sum of components may not equal the total due to rounding.
- Data series are subject to restatement, based on corrections or the receipt of additional information.

INTRODUCTION

UK FINANCE

Amid a rapidly changing landscape, 2021 was a year that more than ever highlighted the need for collaborative action to effectively address the epidemic of fraud in the UK.

The lockdown may be over, but the enduring effects of the Covid-19 pandemic continue to have a significant impact on families and businesses across the UK. Fraudsters have become increasingly adept at adapting their methods to suit changes in our lifestyles and in consumer behaviour. We can only tackle this through effective coordinated action, and we need continued efforts from government and other sectors to tackle what is now a national security threat.

Most notable is the rise in impersonation scams and in authorised push payment (APP) fraud overall. In 2021 communications regulator Ofcom found that eight out of ten people that were surveyed had been targeted with scam texts or phone calls, intended to convince them that they were from trusted organisations such as banks, the NHS or government departments.

The majority of APP fraud starts with some type of social engineering. As well as scam texts, phone calls and emails, more and more of us are paying for goods and services remotely. Fraudsters have become adept at convincing online users to divulge key personal or financial information. Criminals continue to take advantage of people's doubts and fears to trick victims into handing over personal details and passwords with which they can then use to access financial accounts or set up fake ones. Equally, this information is also subsequently used to dupe the victim into authorising payments to the criminal's account.

Methods include manipulating social media users, fake websites that impersonate known brand names, and impersonating utility services and home delivery services. Most people will have received an email or a text for a parcel they didn't order or a broadband provider they don't have, with instructions to 'click here to check your account'.

Since 2019, the APP voluntary code has been in place and hundreds of millions of pounds has been reimbursed to thousands of customers who have fallen victim to fraud. The government has said it will legislate in the upcoming Financial Services and Markets Bill to enable regulatory action by the Payment Systems Regulator (PSR) on APP fraud, with the PSR due to issue a consultation on APP reimbursement later this year. We have long called for a regulated code, backed by legislation, to ensure consumer protections apply consistently and so welcome this move by the government.

Of course, it is not just about reimbursement. Fraud has a devastating impact on victims – and the money stolen funds serious organised crime, as well as impacting the wider economy. We need a coherent, agreed message with government, law enforcement, telecommunications, financial services and tech sectors collaborating together to tackle the problems at source. The banking and finance sector has been at the forefront of cross-sector collaboration and data sharing in the past year, and we have seen a number of successes. We saw the inclusion of user generated fraud into the Online Safety Bill, and we welcomed seeing the scope of the Bill expanded earlier this year to include advertising on social media and search engines, something we have long been calling for.

Our Industry Fraud and Scams Strategy calls for action by all stakeholders involved in the customer journey. It is vital that the industry works together with regulators and legislators to improve current payment processes and ensure that new systems have fraud prevention as an intrinsic part of their design.

Major online platforms – search engines, social media and shopping platforms – are the gateway to almost all online activity and they must provide a barrier to fraud and not a conduit. We believe that collaboration with telecommunications and technology stakeholders will help us develop a comprehensive approach to stem the flow of fraud. The Online Fraud Steering Group (OFSG), co-chaired by UK Finance chief executive David Postings, together with TechUK and the National Economic Crime Centre (NECC), was set up in April 2021. It brings together major representatives from the tech and digital sectors, as well as UK Finance members, to drive progress among all stakeholders in combating fraud initiated online.

It isn't just about big tech, though. The Banking Protocol, the industry's rapid scam response scheme initiative in which frontline bank staff work with the police to identify and help potential fraud victims, prevented £60.7 million of fraud in 2021, 34 per cent more than in 2020. Its success highlights the importance of joint work between the police and the banking and finance industry to protect customers and tackle criminals.

Our Dedicated Card and Payment Crime Unit (DCPCU), an operational police unit funded by and working with UK Finance members, has been hugely successful in its collaborative work with banks, social media companies, the telecoms sector and government to bring criminals to justice and prevent fraud. The unit prevented a record £101 million from being stolen in 2021, the highest amount in the unit's 20-year history. Meanwhile, last August many of the world's major technology companies pledged to support Take Five to Stop Fraud, our anti-fraud campaign, with $1 million worth of advertising.

The Economic Crime and Corporate Transparency Bill announced in the Queen's Speech in May this year highlighted the importance of greater information sharing. The Bill promises greater enforcement powers to address money laundering. In addition, having the legislative framework to be able to slow down some faster payments should give banks greater flexibility over whether to make or accept payments if there is enough suspicion of fraud. The industry has also been working with the Home Office on the next Economic Crime Plan, and through the Joint Fraud Taskforce on a proposed ten-year fraud strategy.

The challenges we face are clear. Criminal gangs, well-organised, ruthless and technology-savvy, are not going to be discouraged easily. They are systemically bypassing banks security measures by directing their efforts at the customer outside the payments journey. This highlights how important it is for different sectors to work together to fight fraud. It is an ever growing and persistent threat to businesses, consumers and the economy as a whole. The banking and finance industry continues to invest billions in tackling fraud. But it is only through this coordinated action that we will really be able to shift the dial.

Katy Worobec
Managing Director,
Economic Crime,
UK Finance

INTRODUCTION

LEXISNEXIS® RISK SOLUTIONS

LexisNexis® Risk Solutions is proud to once again sponsor this year's fraud report by UK Finance. The information within this report is corroborated by the data and trends within our latest Cybercrime Report[1], which shows macro and regional fraud trends.

2021 was something of a stop-start year for UK consumers. However, with the UK economy growing at its fastest rate since the Second World War and consumer uncertainty decreasing as lockdowns eased, it fast became an opportune year to commit fraud. 64 billion transactions were monitored by the LexisNexis® Digital Identity Network[2] in 2021, with Account Logins seeing the highest growth in volumes, as the previous year's new-to-digital population become increasingly reliant on digital banking.

Globally we see an increase in transactions of 51 per cent for the financial industry, while the UK saw growth of 11 per cent, on top of an already well-established digital base. UK financial institutions are continuing to double down on their mobile app strategies, with 89 per cent of UK financial services transactions executed on mobile.

UK consumers are now extremely comfortable transacting on mobile and banks are continuing to optimise the balance between excellent in-app customer experience and fraud prevention. Our research shows internet banking via app still seems to be the safest way to transact in the UK, thanks to the implementation of various authentication and prevention strategies. However, as banks continue to expand their digital capabilities to retain existing customers and attract new, younger ones, this approach will need to be built upon, as mobile will give fraudsters an even greater attack surface in the future.

Over the past year, sophisticated and targeted social engineering scams have attracted increasing attention within the mainstream media, as they continue to impact a wide range of customers across all ages – in particular the younger and older groups. Among the most pernicious and prevalent are bank employee impersonation, romance and investment scams.

Although scams are currently the number one issue, organisations are now looking at utilising advanced technological capabilities, such as behavioural biometrics and advanced machine learning in combination with real-time insight data to help detect and identify scams whie in progress. At LexisNexis Risk Solutions we are helping the industry in tackling

[1] Download the latest LexisNexis Risk Solutions' Cybercrime Report: https://risk.lexisnexis.co.uk/insights-resources/research/cybercrime-report

[2] LexisNexis® Digital Identity Network® is the world's largest network of digital identities, bringing together global crowdsourced intelligence from over 60 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

these challenges, being at the forefront of innovation and investing heavily in market-leading behavioural biometrics solutions.

Password resets are also emerging as a new focal point for fraud within the customer journey, our data shows. Growth in attacks on password resets has accelerated globally in 2021, with one in every eight password reset attempts being an attack in H2 2021, up from one in 50 in H1 2020. Fraudsters are constantly looking for ways to infiltrate the customer journey via the weakest point, in this case locking out the genuine customer and appropriating their funds.

We continue to monitor the strong cross-industry fraud links as fraudsters' attack patterns increasingly focus on multiple industries to commit fraud. In one example the Cybercrime Report profiled a prolific fraudster who attacked the Communication, Mobile, Media (CMM), e-commerce, financial services and insurance industries all within 28 days, using different methods to commit fraud. With this behaviour becoming increasingly commonplace, fraud links between industries must continue to be strengthened.

Fraud is now truly global and industry agnostic. LexisNexis® Risk Solutions strongly emphasises the need for intra- and inter-industry collaboration when it comes to detecting fraud. Informed by these latest fraud trends and macro-economic intelligence, banks and the wider financial services eco-system must collectively move to secure every point in their customer journey and stop the fraudsters that would otherwise exploit their vulnerabilities.

Pratik Choudhary
Manager, Fraud & Identity,
LexisNexis® Risk Solutions

TRENDS AND STATISTICS

2021 OVERVIEW

Unauthorised financial fraud losses across payment cards, remote banking and cheques totalled £730.4 million in 2021, a decrease of seven per cent compared to 2020.

Banks and card companies prevented £1.4 billion in unauthorised fraud in 2021. This represents incidents that were detected and prevented by firms and is equivalent to 65.3p in every £1 of attempted fraud being stopped.

In addition to this, UK Finance members reported 195,996 incidents of Authorised Push Payment (APP) scams in 2021 with gross losses of £583.2 million, compared with £420.7 million in 2020.

BEHIND THE FRAUD FIGURES

The continuing impact of Covid-19 has reshaped the fraud landscape in the past 18 to 24 months. The pandemic has resulted in certain types of fraud falling while others have risen.

Criminals continue to adapt the methods they use to try and trick consumers into handing over account details, or personal information that can be used to defraud them of their funds.

They typically employ a range of techniques to trick victims into allowing them to access personal and financial information, such as their internet banking One Time Passcodes and log in details, that can be used to steal from consumers. While it is not possible to be specific about the values that can be attributed to individual methods of attack, intelligence reported by our members highlights the main drivers.

Social engineering, in which criminals groom and manipulate people into divulging personal or financial details or transferring money, continued to be the key driver of both unauthorised and authorised fraud losses in 2021.

Throughout the year, criminals focused their activity on authorised push payment (APP) fraud, where the customer is tricked into authorising a payment to an account controlled by a criminal. Using tactics such as scam phone calls, text messages and emails, as well as fake websites and social media posts, criminals seek to trick people into handing over personal details and passwords. This information is then used to target victims and convince them to authorise payments. The majority of authorised push payment fraud starts online.

While the amount lost in APP fraud has outweighed card fraud, the latter is still very a major issue albeit in lower numbers. Payment card fraud losses, such as remote purchase (card not present or CNP), counterfeit, lost and stolen, card not received and card ID theft, fell seven per cent in 2021 while the number of actual case volumes remained broadly the same as before.

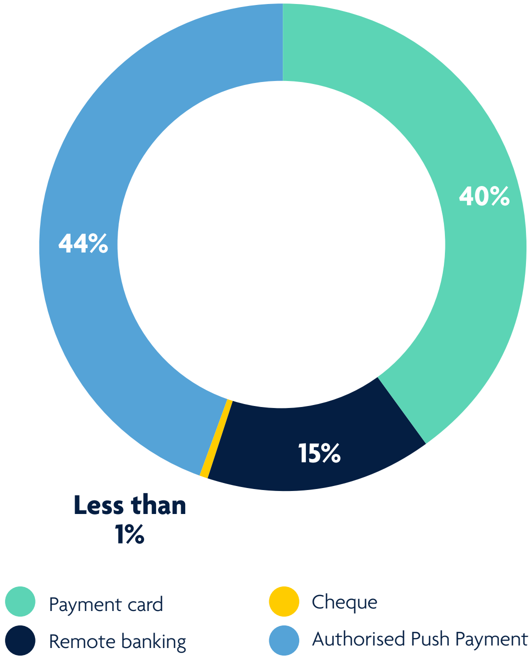
With more of us working from home, spending longer online, and doing more internet shopping, criminals have been able to target people directly in their homes across online platforms. This is likely to have made people more susceptible to these scams. There has also been a spike in money mule activity, investment, delivery and purchase scams over the last year.

Smishing and phishing fraud took advantage of people's vulnerability while at home and needing to access new or unfamiliar online services rather than to do it person. While customers of all age groups are falling victim to these scams, it is younger age groups that are often the prime target.

Our research found that people under 35 are more likely than older age groups to have been targeted in an impersonation scam and be swayed to provide personal or financial information. These are often long-term scams in which a criminal will contact you pretending to be a person or organisation you trust.

Romance scams are a key example of this 'stealth' fraud, where a criminal pretends to develop a relationship with the victim in order to persuade them to transfer/give access to money. Through our Take Five campaign, we continue to urge consumers to be suspicious of requests for money from someone they have never met in person, particularly if they have only recently met online.

Total 2021 financial fraud losses by type
% of total



THE INDUSTRY RESPONSE

The banking and finance industry is working hard to protect customers from fraud and scams, while partnering with government, law enforcement and the private sector 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 £1.4 billion of unauthorised fraud in 2021, equivalent to 65.3p in every £1 of attempted unauthorised fraud being stopped without a loss occurring.
- Working with the government and law enforcement to establish clear strategic priorities, improve accountability and coordination through the Economic Crime Strategic Board (ECSB), jointly chaired by the home secretary and the chancellor. The ECSB has agreed a number of public private priorities, with a focus on Suspicious Activity Reports (SARs) Reform, work on legislative proposals and effectiveness and efficiency.
- Advocating for economic crime to be fully included within the Online Safety Bill. We welcome the expansion the scope of the Online Safety Bill to include advertising on social media and search engines.
- The jointly published Home Office and UK Finance Economic Crime Plan sets out how to better harness the combined capabilities of the public and private sectors to make the UK a leader in the global fight against economic crime. The industry is working with the government on a new Economic Crime Plan and Ten Year Fraud Strategy. The Economic Crime and Corporate Transparency Bill announced in the Queen's Speech in May 2022 will support this by providing a framework for all sectors working together.
- Sharing intelligence on emerging threats with law enforcement, government departments and regulators through the National Economic Crime Centre. This drives down serious organised economic crime, protecting the public and safeguarding the prosperity and reputation of the UK as a financial centre.
- Sharing intelligence across the banking and finance industry on emerging threats, data breaches and compromised card details via UK Finance's Intelligence and Information Unit (I&I Unit). In 2021, 1.6 million compromised card numbers were received through law enforcement and disseminated via the I&I unit to enable card issuers to take the necessary precautions to protect customers. The industry has proposed new powers on information and intelligence sharing to make it easier for regulated sector firms to share information with each other.
- Delivering customer education campaigns to help them stay safe from fraud, spot the signs of a scam, and to prevent consumers being duped by criminals. These include our Take Five to Stop Fraud and Don't Be Fooled campaigns. 34 major banks and building societies have signed up to the Take Five Charter, bringing the industry together to give people simple and consistent fraud awareness advice.

- Training staff to spot and stop suspicious transactions. The Banking Protocol rapid response scheme allows branch staff at banks, building societies and Post Offices to alert the police when they think a customer is being scammed, whether in branch, on the telephone, or online banking. The Banking Protocol has prevented £202.8 million in fraud and led to 1,005 arrests since it launched in 2016. In 2021 £60.7 million was stopped through the scheme, 34 per cent more than in 2020.
- 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 2021 the DCPCU prevented a record £101 million from being stolen in 2021, the highest amount in the unit's 20-year history, arrested 123 suspected fraudsters and secured 83 convictions.
- Working with the regulator Ofcom to crack down on number spoofing, including the development and enhancements of the 'do not originate' list. This work has led to significant successes in preventing criminals from spoofing the phone numbers of trusted organisations such as the numbers on the back of bank cards.
- Working with text message providers and law enforcement to block scam text messages including those exploiting the Covid-19 crisis. 2098 unauthorised sender IDs are currently being blocked to prevent them being used to send scam text messages mimicking trusted organisations, including over 450 related to Covid-19.

TECHNOLOGY

The banking industry continues to proactively use 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 such as 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, meaning 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.

In March 2022, requirements for Strong Customer Authentication (SCA) in the context of e-commerce took effect. SCA rules, aimed at reducing fraud by verifying a customer's identity, require all payment providers to use multi-factor authentication for higher value and higher risk online transactions.

The Industry Fraud and Scams Strategy encourages collaboration with telecommunications and technology stakeholders to assess and close down vulnerabilities across the wider ecosystem, including upstream in the customer journey. It is working on technical developments to enable Payment Service Providers to manage risk more effectively.

To combat telephone banking fraud, some banks are using technology which allows them to identify the different sound tones 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.

CARD FRAUD

DEBIT, CREDIT, AND OTHER PAYMENT CARD FRAUD

VALUE	£524.5m	- 7%	VOLUME	2,823,202	0%

Fraud losses on UK-issued cards totalled £524.5 million in 2021, a seven per cent fall from £574.2 million in 2020. At the same time, total spending on all debit and credit cards reached £838 billion in 2021, with 22.9 billion transactions made during the year.

Overall card fraud losses as a proportion of the amount we spent on our cards during 2021 was 6.3p per £100 spent.

A total of £966.6 million in card fraud was stopped by banks and card companies in 2021. This is equivalent to 64.8p in every £1 of attempted 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 fully refund customers in excess of 98 per cent of all confirmed 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. In March 2022, requirements for Strong Customer Authentication (SCA) in the context of e-commerce took effect. SCA rules are aimed at reducing fraud by verifying a customer's identity when they make certain higher value online purchases.
- 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 groups responsible for financial fraud and scams. Throughout 2021, the unit prevented a record £101 million of fraud in 2021, the highest amount in the unit's 20-year history.

Fraud Type (£m)	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	% Change 20/21
Remote Purchase (CNP)	£247.3	£301.0	£331.5	£398.4	£432.3	£408.4	£506.4	£470.2	£452.6	£412.5	-9%
Of which e-commerce	£139.6	£140.2	£190.1	£219.1	£261.5	£310.3	£310.4	£360.5	£377.2	£339.2	-10%
Counterfeit	£42.3	£43.3	£47.8	£45.7	£36.9	£24.2	£16.3	£12.8	£8.7	£4.7	-46%
Lost & Stolen	£55.4	£58.9	£59.7	£74.1	£96.3	£92.9	£95.1	£94.8	£78.9	£77.2	-2%
Card ID Theft	£32.6	£36.7	£30.0	£38.2	£40.0	£29.8	£47.3	£37.7	£29.7	£26.3	-12%
Card non-receipt	£12.8	£10.4	£10.1	£11.7	£12.5	£10.2	£6.3	£5.2	£4.4	£3.9	-11%
Total	£390.4	£450.2	£479.0	£568.1	£618.1	£565.4	£671.4	£620.6	£574.2	£524.4	-7%
UK	£288.4	£328.2	£328.7	£379.7	£417.9	£407.5	£496.6	£449.9	£414.5	£384	-7%
Fraud Abroad	£102.0	£122.0	£150.3	£188.4	£200.1	£158.0	£174.8	£170.7	£159.7	£140.5	-12%

CARD FRAUD VOLUMES

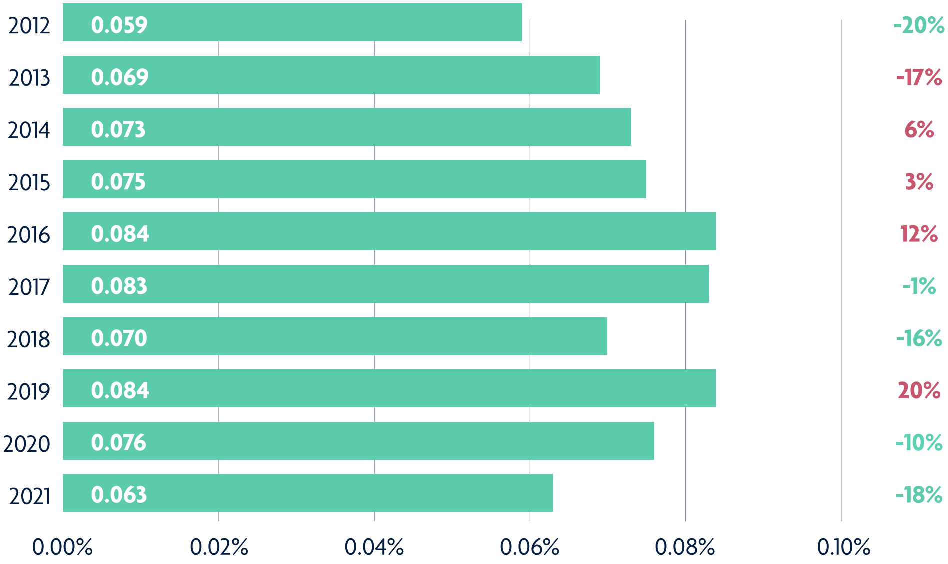
UK Finance also publishes the number of fraud incidents to convey more fully the dynamics of the fraud environment in the UK. The number of confirmed cases of card fraud (2.82 million) reported during 2021 fell very slightly in comparison to the number reported in 2020 (2.84 million). The average case value for a card fraud has fallen from £339 in 2016 to just under £186 in 2021. This demonstrates that cases are being spotted and stopped by card issuers more quickly, meaning that organised criminals must commit more frauds to to steal the same amount of money.

Remote purchase (CNP) accounts for the biggest proportion of card fraud with 86 per cent of all card fraud cases reported involving the use of stolen card details to buy something on the internet, over the phone or through mail order. There was a slight rise in the number of cases involving remote purchase fraud in 2021. Cases of counterfeit cards have fallen to the lowest ever levels reported mainly due to Chip & PIN, but also in more recent times due to the restrictions in movement because of the pandemic.

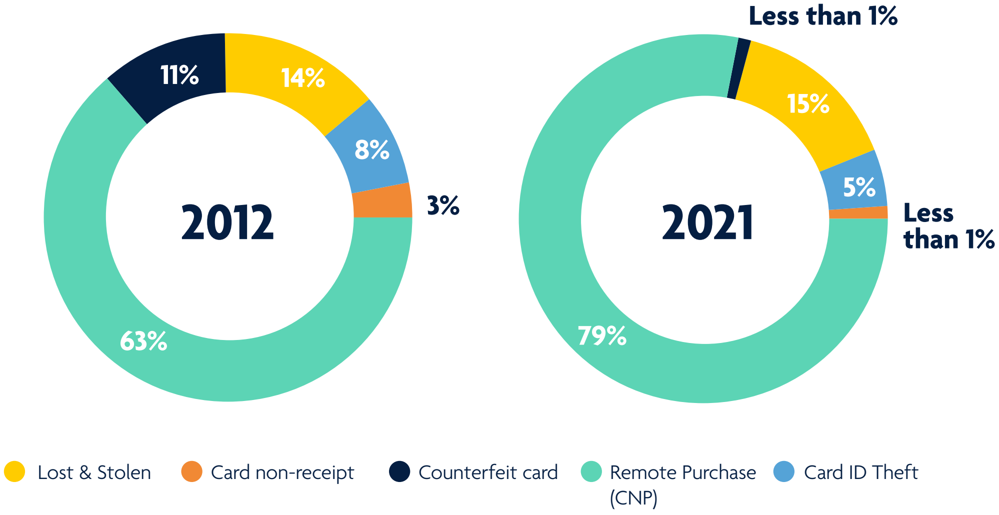
It is important to note that the number of cases relates to the number of accounts that have been defrauded, as opposed to the number of victims.

Fraud Type	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	% Change 20/21
Remote Purchase (CNP)	752,450	951,998	1,019,146	1,113,084	1,437,832	1,398,153	2,050,275	2,157,418	2,417,866	2,423,826	0%
Counterfeit	98,555	101,109	99,279	86,021	108,597	85,025	58,636	65,907	52,782	24,908	-53%
Lost & Stolen	113,162	138,967	133,943	143,802	231,164	350,279	434,991	460,142	321,994	325,501	1%
Card ID Theft	24,287	30,718	26,542	33,566	31,756	29,156	63,791	54,165	34,545	40,026	16%
Card non-receipt	9,053	9,125	9,302	10,719	11,377	10,903	10,046	7,907	8,435	8,941	6%
TOTAL	**997,507**	**1,231,917**	**1,288,212**	**1,387,192**	**1,820,726**	**1,873,516**	**2,617,739**	**2,745,539**	**2,835,622**	**2,823,202**	**0%**

Fraud to turnover ratio 2012-2021



Card fraud losses 2021 split by type (as a percentage of total losses)



REMOTE PURCHASE

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

VALUE	£412.5m	- 9%	VOLUME	2,423,826	0%

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 £412.5 million in 2021, a decrease of nine per cent when compared to 2020. Online fraud against UK retailers totalled an estimated £238.6 million in 2021, a decrease of nine per cent from £263.1 million on the previous year. Mail and telephone order (MOTO) fraud against retailers based in the UK increased by two per cent from £64.3 million on the previous year.

Overall card fraud losses for 2021 are lower than in 2020. However, levels remain high as fraudsters continue to exploit the significant rise in online card spending during the pandemic. Despite this, the static nature of the number of cases of remote purchase fraud when compared with a nine 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. Typical examples include third-party data breaches via phishing emails and scam text messages.

Criminals are also taking advantage of the increasing tendency for online shoppers to search for discounted items on social media. When a customer goes to buy the product advertised on a 'fake' social media profile, the criminal uses stolen card details to purchase the item from a legitimate source and then keeps the payment from the customer.

"Digital skimming" is another method criminals use 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.

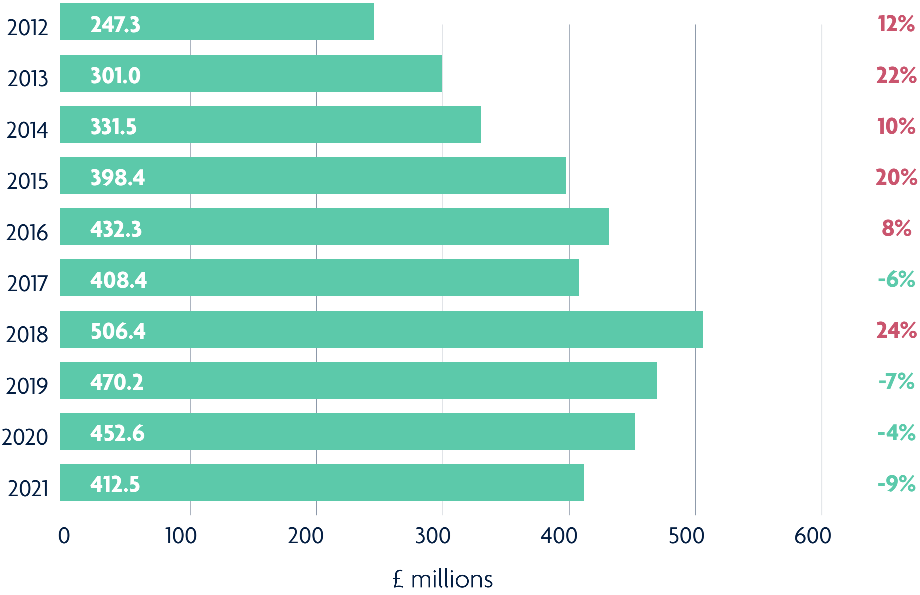
In March 2022, requirements for Strong Customer Authentication (SCA) in the context of e-commerce took effect. This follows the managed programme which UK Finance led on behalf of members in order to ensure an orderly migration to SCA. SCA rules are aimed at reducing fraud by verifying a customer's identity when they make certain higher value online purchases.

In an attempt to circumvent these additional protections, criminals are increasingly using socially 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.

One Time Passcodes (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 or purchase you're about to make.

If you receive a code you weren't expecting, contact your bank immediately on a number you know to be correct, such as the one listed on the back of your debit or credit card.

Remote purchase (CNP) gross fraud losses (UK-issued cards) 2012 – 2021



Remote purchase (CNP) case volumes (UK-issued cards) 2012 – 2021

Year	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Cases	752,450	951,998	1,019,146	1,113,084	1,437,832	1,398,153	2,050,275	2,157,418	2,417,866	2,423,826
Change	6%	27%	7%	9%	29%	-3%	47%	5%	12%	0%

How to stay safe from remote purchase fraud:

If you're using an online retailer for the first time, always take time to research them before you give them any of your details. Be prepared to ask questions before making a payment.

- Trust your instincts – if an offer looks too good to believe then it probably is. Be suspicious of prices that are unfeasibly low.
- Only use retailers you trust, for example, ones you know or have been recommended to you. If you're buying an item made by a major brand, you can often find a list of authorised sellers on their official website.
- Take the time to install the built-in security measures most browsers offer.

COUNTERFEIT CARD FRAUD

VALUE **£4.7m** **- 46%**

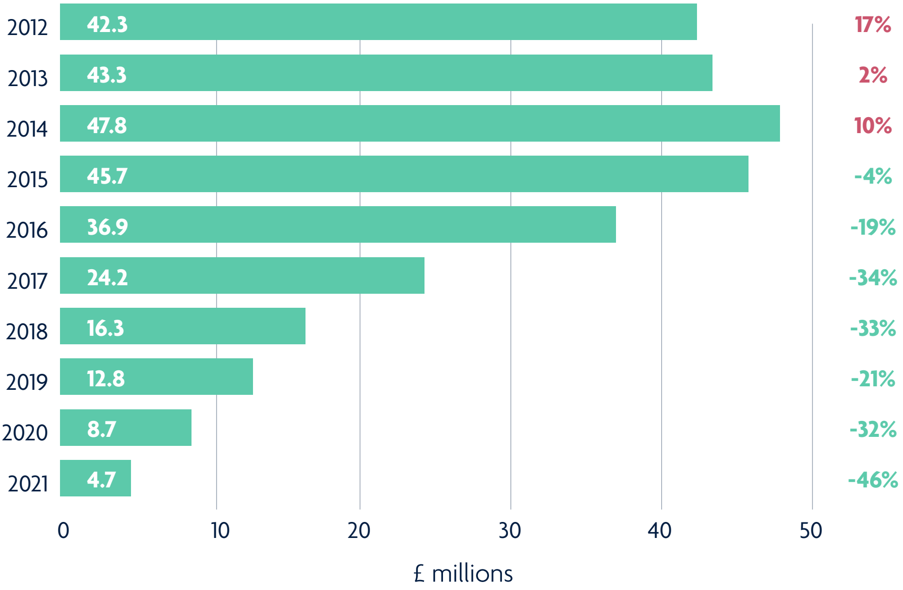
VOLUME **24,908** **- 53%**

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

Counterfeit card losses totalled £4.7 million in 2021, a fall of 46 per cent compared to 2020, the seventh consecutive year a decrease has been reported and 97 per cent lower than the peak in 2008 (£169.8 million). Case volumes more than halved, reducing by 53 per cent to just under 25,000. Both gross losses and case volumes have fallen to the lowest totals on record for this type of fraud.

To obtain the data required to create a counterfeit card, criminals attach concealed or disguised devices to the card-reader slots of ATMs and unattended payment terminals (UPTs), such as self-service ticket machines at railway stations, cinemas, and car parks. The counterfeit cards are typically used overseas in countries yet to upgrade to Chip and PIN. The significant decrease in this type of fraud since 2008 is likely to be a result of the introduction of chip technology in the UK and its subsequent increased adoption around the world, most notably in the United States. The travel restrictions resulting from the Covid-19 pandemic have reduced these opportunities even further and driven down this type of fraud to the lowest level recorded.

Counterfeit card fraud losses (UK-issued cards) 2012 – 2021



Counterfeit card case volumes (UK-issued cards) 2012 – 2021

Year	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Cases	98,555	101,109	99,279	86,021	108,597	85,025	58,636	65,907	52,782	24,908
Change	22%	3%	-2%	-13%	26%	-22%	-31%	12%	-20%	-53%

How to stay safe from counterfeit card fraud:

- Always protect your PIN by fully covering the keypad with your free hand or purse.
- If you spot anything suspicious at an ATM or unattended payment terminal, or someone is watching you, then do not use the machine and report it to your bank.
- Check your statements regularly and if you spot any payments, you don't recognise then contact your card company immediately.

LOST AND STOLEN CARD FRAUD

VALUE	£77.2m	- 2%

VOLUME	325,501	+ 1%

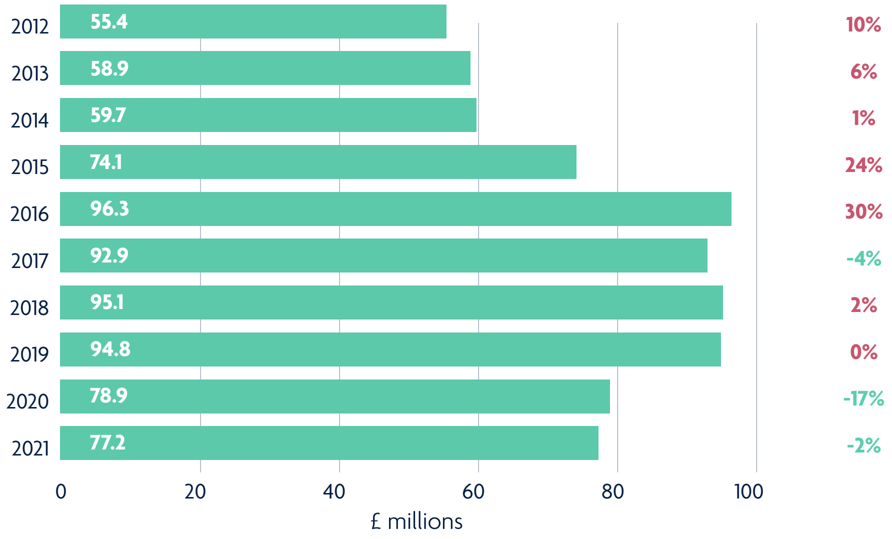
This fraud occurs when a criminal uses a lost or stolen card to make a purchase or payment (whether remotely or face-to-face) or takes money out at an ATM or in a branch.

Losses due to lost and stolen card fraud reduced by two per cent in 2021, falling to £77.2 million compared to £78.9 million in 2020. The number of incidents increased slightly, rising by one per cent over the same period. A rise in the number of incidents was expected during 2021, given the increased opportunities for cards to be lost or stolen in comparison to 2020 when lockdown played a significant role in those opportunities being reduced.

Much of this type of fraud occurs using cards obtained through low-tech methods such as distraction thefts and entrapment devices attached to ATMs.

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 that 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.

Lost and stolen card fraud losses (UK-issued cards) 2012 – 2021



Lost & stolen card case volumes (UK-issued cards) 2012 – 2021

Year	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Cases	113,162	138,967	133,943	143,802	231,164	350,279	434,991	460,142	321,994	325,501
Change	8%	23%	-4%	7%	61%	52%	24%	6%	-30%	1%

How to stay safe from lost and stolen fraud:

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

CARD ID THEFT

VALUE	£26.3m	- 12%	VOLUME	40,026	+ 16%

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 12 per cent in 2021, to £26.3 million. There was however a rise in the number of cases, increasing by 16 per cent to just over 40,000.

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.

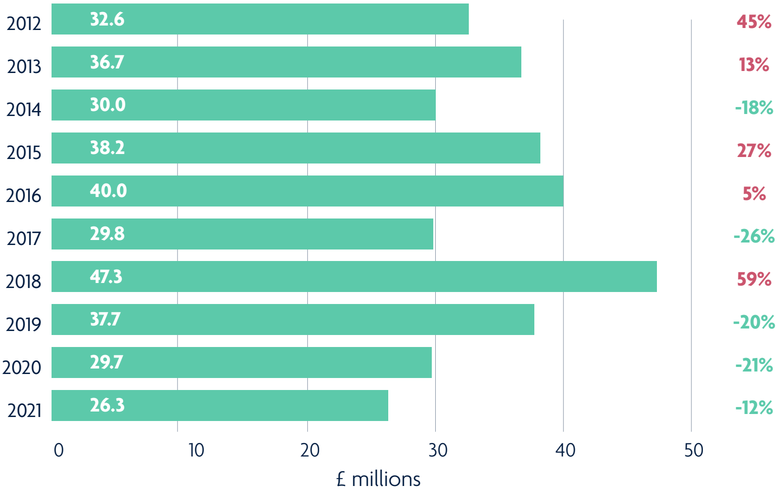
Application fraud - £10.9 million (-28%)

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 - £15.4 million (5%)

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

Card ID theft fraud losses (UK-issued cards) 2012 – 2021



Card ID theft case volumes (UK-issued cards) 2012 – 2021

Year	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Cases	24,287	30,718	26,542	33,566	31,756	29,156	63,791	54,165	34,545	40,026
Change	58%	26%	-14%	26%	-5%	-8%	119%	-15%	-36%	16%

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 you have business 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	£3.9m	- 11%

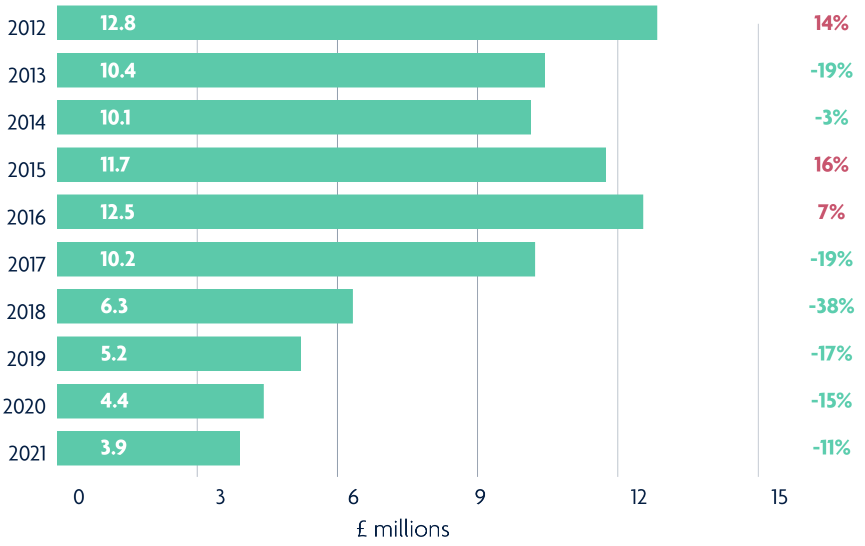
VOLUME	8,941	6%

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 11 per cent in 2021 to £3.9 million. However, the volume of cases rose by six per cent, indicating that measures put in place to detect such frauds early on are having a beneficial effect.

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 (UK-issued cards) 2012-2021



Card not received fraud case volumes (UK-issued cards) 2012 – 2021

Year	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Cases	9,053	9,125	9,302	10,719	11,377	10,903	10,046	7,907	8,435	8,941
Change	6%	1%	2%	15%	6%	-4%	-8%	-21%	7%	6%

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	£46.8m	- 4%

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 four per cent in 2021 to £46.8 million. Given the extended periods in 2021 when many shops were closed due to Covid-19 restrictions, this has contributed to reducing cases of such fraud.

Much 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.

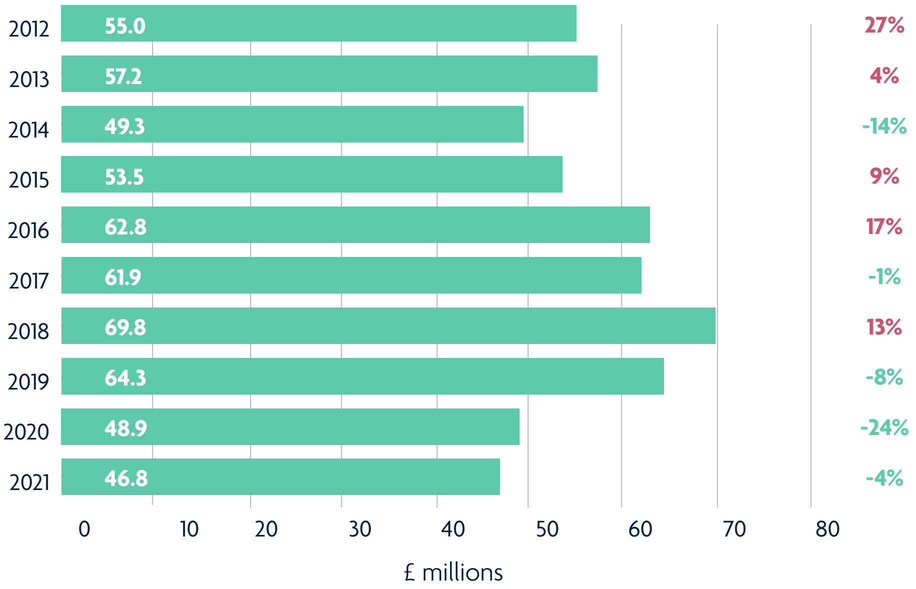
This category includes fraud incidents involving the contactless functionality on both payment cards and mobile devices. Contactless fraud on payment cards and devices totalled £19.1million in 2021, a rise of 20 per cent when compared to 2020. However, it should be noted that 2020 saw the first annual decrease in contactless losses since we began collecting data, due in part to the reduced opportunities for fraudsters to commit these types of scams because of lockdown restrictions during the pandemic.

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.

Overall spend on contactless cards was £166 billion in 2021 compared to 2020 with spending of £114 billion; a rise of 46 per cent.

This means fraud is equivalent to 1.2p in every £100 spent using contactless technology, a reduction in the total recorded in 2020 (1.4p). Contactless fraud on payment cards and devices represents less than four per cent of overall card fraud losses, while 57 per cent of all card transactions were contactless last year.

Card Fraud Losses at UK retailers (face-to-face transactions) 2012-2021



INTERNET/E-COMMERCE FRAUD

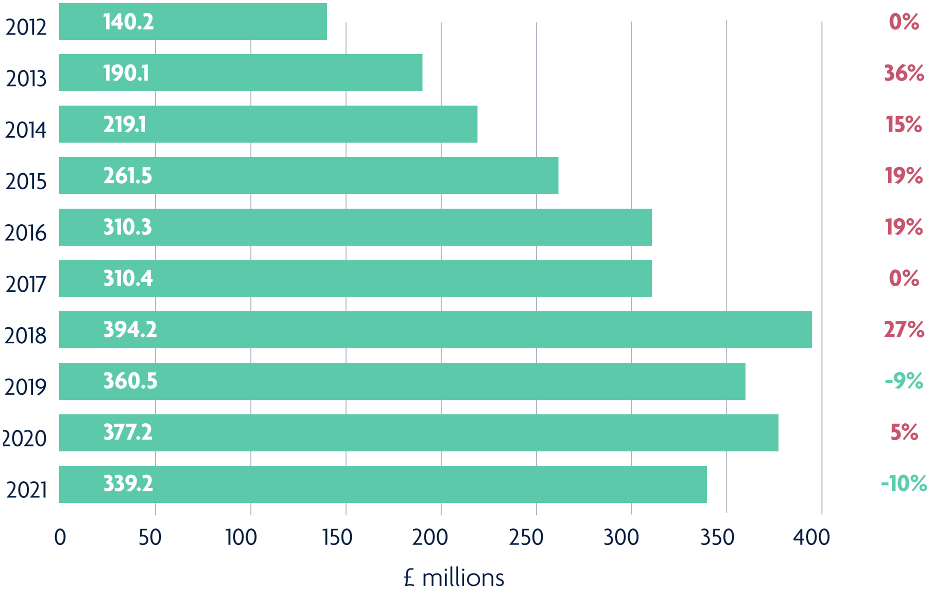
VALUE	£339.2m	- 10%

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 £339.2 million of e-commerce fraud took place on cards in 2021, accounting for 65 per cent of all card fraud and 82 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 2012-2021



CARD FRAUD AT UK CASH MACHINES

VALUE £24.4m - 13%

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. Most losses result from distraction thefts which occur mainly in shops, bars and restaurants and at ATMs.

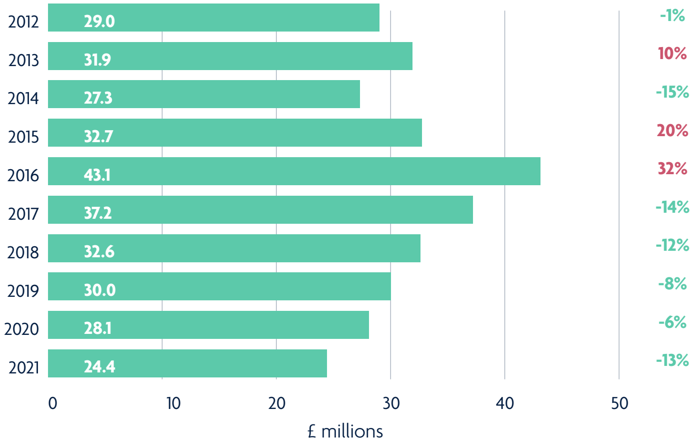
Fraudsters also target cash machines to compromise or steal cards or card details in three main ways:

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 2012-2021



CARD FRAUD ABROAD

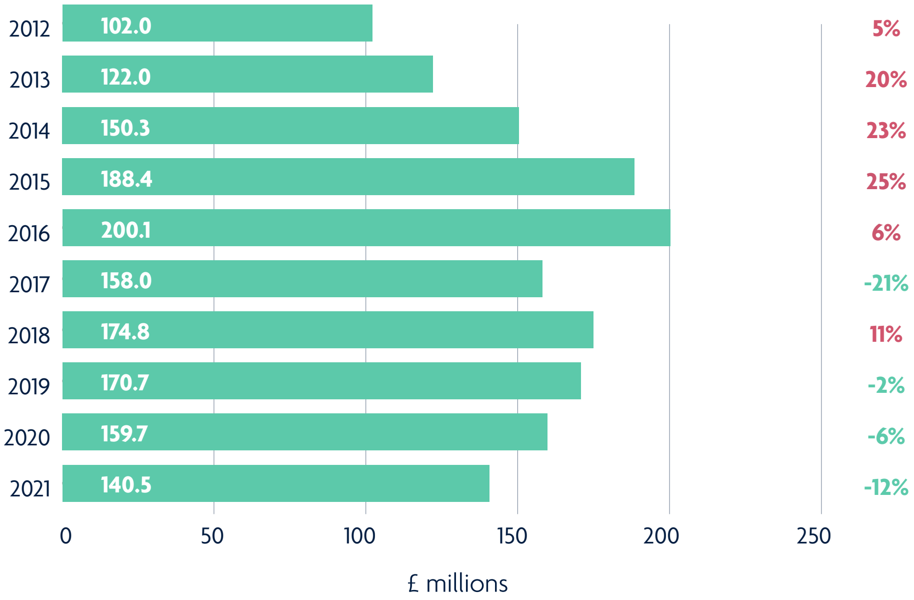
VALUE £140.5m - 12%

This category covers fraud occurring in locations overseas on UK-issued cards. The majority (78 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.

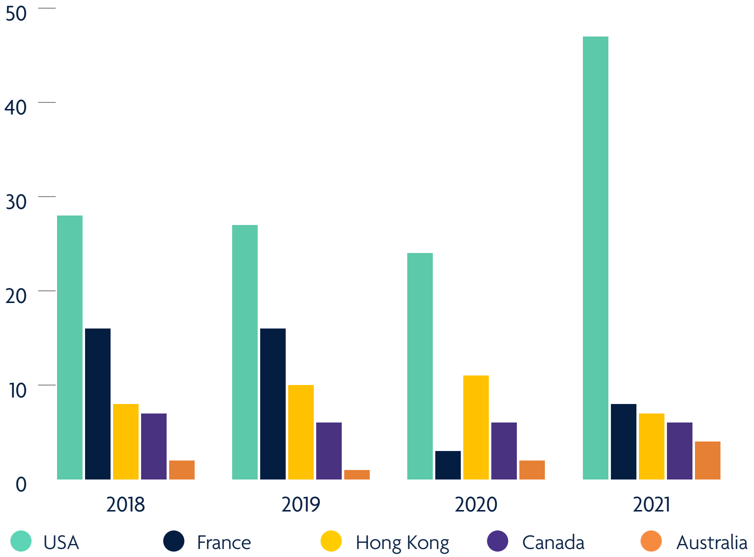
International fraud losses for 2021 were £140.5 million, compared with losses at their peak in 2008 of £230.1 million, a decrease of 39 per cent.

International Fraud Losses 2012 – 2021



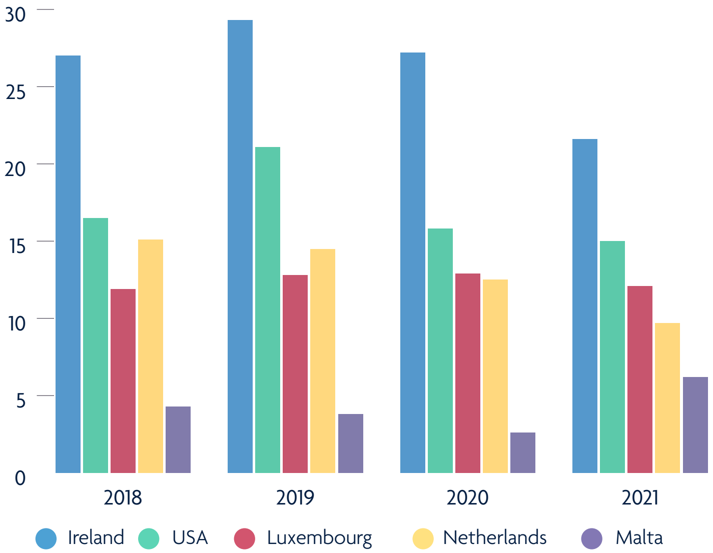
Top five countries for fraud on foreign-issued cards occurring in the UK 2017-2021

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 2017-2021

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



CHEQUE FRAUD

CHEQUE FRAUD

VALUE	£6.4m	- 48%

VOLUME	815	- 35%

Cheque fraud losses fell to £6.4 million in 2021, down from £12.3 million in 2020. Meanwhile the volume of fraudulent cheques decreased by 35 per cent. The fall in cheque fraud is likely to have been driven by the continued fall in the use of cheques.

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.

A total of £33 million of cheque fraud was prevented in 2021, a fall of 86 per cent on 2020 and further evidencing the overall reduction in cheque fraud seen in recent years.

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

Counterfeit cheque fraud - £2.6 million (-63%)

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 - £1.6 million (-11%)

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, for example by altering the beneficiary's name or the amount of the cheque.

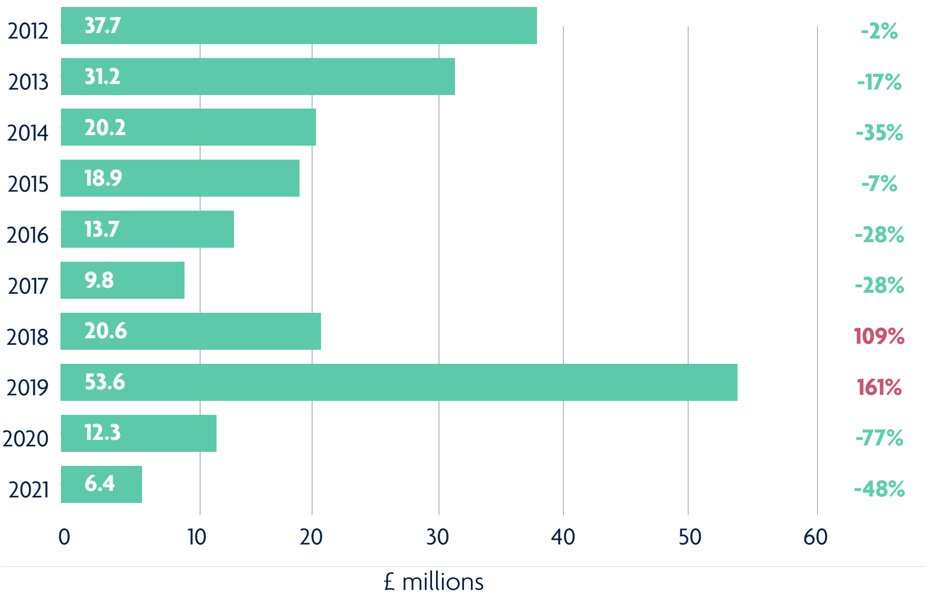
Forged cheque fraud – £2.2 million (-34%)

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

Prevented cheque fraud 2015 – 2021

Cheque	2015	2016	2017	2018	2019	2020	2021	% Change 20/21
Prevented Value	£392.8m	£196.2m	£212.3m	£218.2m	£550.8m	£238.5m	£33.1m	-86%

Cheque Fraud losses 2012-2021



Annual case volumes cheque fraud 2012-2021

Year	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Cases	15,539	10,471	8,168	5,746	3,388	1,745	2,020	2,852	1,247	815
Change	2%	-33%	-22%	-30%	-41%	-48%	16%	41%	-56%	-35%

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's name.
- Keep your chequebook in a safe place, report any missing cheques to your bank immediately.
- Check your statements regularly and if you spot any payments you don't recognise, contact your bank or building society immediately.

REMOTE BANKING FRAUD

REMOTE BANKING FRAUD

VALUE	£199.5m	+ 1%	VOLUME	88,450	+ 20%

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 £199.5 million in 2021, one per cent higher than seen in 2020. The number of cases of remote banking fraud increased by 20 per cent to 88,450. 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 2021, 86 per cent of the adult population used at least one form of remote banking.

Restrictions on movement and an increase in people working from home – are situations that fraudsters have made every attempt to take advantage of.

A total of £365 million of attempted remote banking fraud was stopped by bank security systems during 2021. This is equivalent to 64.7p in every £1 of fraud attempted being prevented. In addition, 15 per cent (£30.6 million) of the losses across all remote banking channels were recovered after the incident.

Remote banking fraud losses 2012-2021

	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Change
Internet	£57.0m	£58.8m	£81.4m	£133.5m	£101.8m	£121.2m	£123.0m	£111.8m	£159.7m	£158.3m	**-1%**
Telephone	£14.7m	£13.1m	£16.8m	£32.3m	£29.6m	£28.4m	£22.0m	£23.6m	£16.1m	£15.5m	**-4%**
Mobile	N/A	N/A	N/A	£2.8m	£5.7m	£6.5m	£7.9m	£15.2m	£21.6m	£25.8m	**19%**
Total	**£73.4m**	**£71.7m**	**£71.9m**	**£98.2m**	**£137.0m**	**£156.1m**	**£152.9m**	**£150.7m**	**£197.3m**	**£199.5m**	**1%**

Annual case volumes remote banking fraud 2012-2021

	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	Change
Internet	16,355	13,799	16,041	19,691	20,088	21,745	20,904	25,849	55,995	72,557	**30%**
Telephone	7,095	5,596	5,578	11,380	10,495	9,577	7,937	11,199	7,490	4,623	**-38%**
Mobile	N/A	N/A	N/A	2,235	2,809	3,424	2,956	6,872	10,155	11,270	**11%**
Total	**23,450**	**19,395**	**21,819**	**33,306**	**33,392**	**34,746**	**31,797**	**43,920**	**73,640**	**88,450**	**20%**

*Mobile banking fraud reporting was not introduced until 2015.

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.
- 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	£158.3m	- 1%	VOLUME	72,557	+ 30%

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 (ISPs) and e-commerce companies. The stolen details are then used to access a customer's online account and to make an unauthorised transaction.

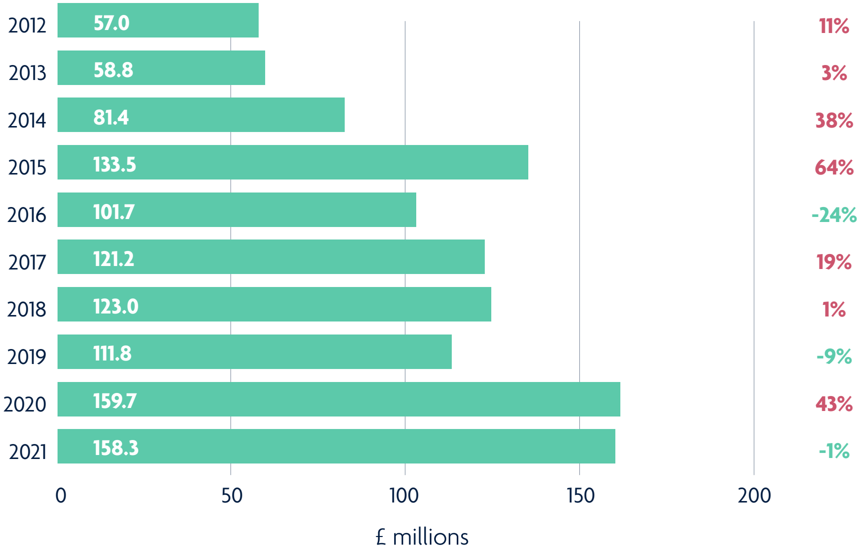
The fact that many people have been working from home, spending longer online, and doing more internet shopping, may have made may them more susceptible to these scams. Intelligence suggests that customers of all age groups are falling victim to these scams, but particularly across younger age groups.

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 or PC.

There has been a rise in the use of phishing websites to obtain customers' online banking credentials. 36,450 bank-branded phishing websites were identified and taken down in 2021, three per cent higher than the previous year.

A total of £314 million of attempted internet banking fraud was stopped by bank security systems during 2021. This is equivalent to 66.5p in every £1 of fraud attempted being prevented. In addition, 16 per cent (£25.7 million) of the losses across the internet banking channel were recovered after the incident.

Internet banking fraud losses 2012-2021



Annual case volumes for internet banking fraud 2012-2021

Year	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Cases	16,355	13,799	16,041	19,691	20,088	21,745	20,904	25,849	55,995	72,557
Change	N/A	-16%	16%	23%	2%	8%	-4%	24%	117%	30%

How to stay safe from internet banking fraud:

- A genuine bank or organisation will never contact you out of the blue to ask for your PIN or full password. Only give out your personal or financial details to use a service 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

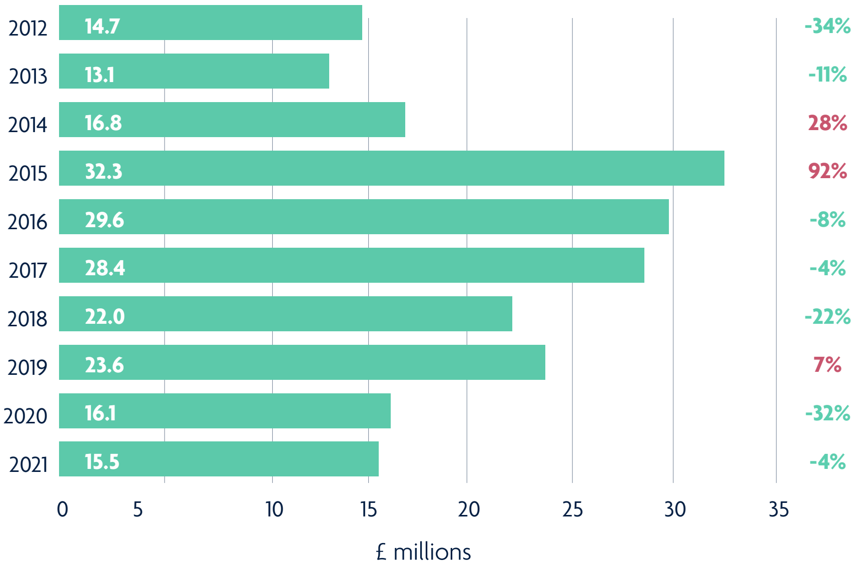
VALUE	£15.5m	- 4%	VOLUME	4,623	- 38%

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 £41.6 million of attempted telephone banking fraud was stopped by bank security systems during 2021. This is equivalent to 72.9p in every £1 of fraud attempted being prevented. In addition, 12 per cent (£1.9 million) of the losses across the telephone banking channel were recovered after the incident.

Telephone banking fraud losses 2012-2021



Annual case volumes for telephone banking fraud 2012-2021

Year	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Cases	7,095	5,596	5,578	11,380	10,495	9,577	7,937	11,199	7,490	4,623
Change	N/A	-21%	0%	104%	-8%	-9%	-17%	41%	-33%	-38%

How to stay safe from telephone banking fraud:

- Never disclose security details, such as your full banking password. A genuine financial provider or organisation will never ask you for these in an email, on the phone or in writing.
- Never give remote access to any of your devices while on a phone call 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), it doesn't mean they are genuine.

MOBILE BANKING FRAUD

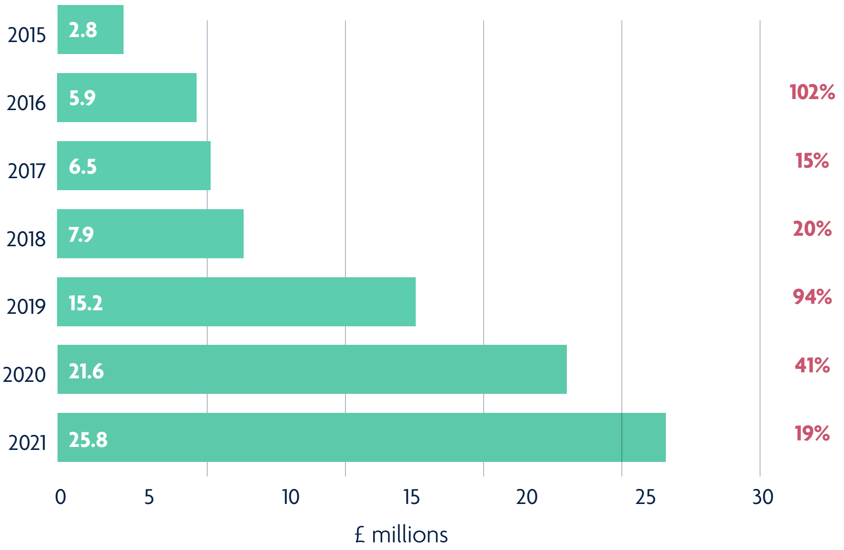
VALUE	£25.8m	+ 19%	VOLUME	11,270	+ 11%

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. At least 57 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 and payment limits increase.

A total of £9.9 million of attempted mobile banking fraud was stopped by bank security systems during 2021. This is equivalent to £27.7p in every £1 of fraud attempted being prevented. In addition, 11 per cent (£3 million) of the losses across the mobile banking channel were recovered after the incident

Mobile banking fraud losses 2015-2021



Annual case volumes for mobile banking fraud 2015-2021

Year	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Cases	N/A	N/A	N/A	2,235	2,809	3,424	2,956	6,872	10,155	11,270
Change	N/A	N/A	N/A	N/A	26%	22%	-14%	132%	48%	11%

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 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 FRAUD

AUTHORISED PUSH PAYMENT (APP) FRAUD

VALUE	£583.2m	+ 39%

VOLUME	195,996	+ 27%

In an authorised push payment scam, a criminal will trick their victim into sending money directly from their account to an account which the criminal controls. Losses due to authorised push payment scams were £583.2 million in 2021. This was split between personal (£505.8 million) and non-personal or business (£77.4 million).

In total there were 195,996 cases. Of this total, 188,964 cases were on personal accounts and 7,032 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 has reached 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.

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.

Update on previous fraud figures

Validation checks we undertook on the fraud data supplied to us prior to publication this year uncovered some issues with historic authorised push fraud (APP) figures. We found that some previously published APP figures had been overstated. Updated figures for the first half of 2021 and the whole 2020 are all included within this report.

We have not included any figures for years prior to 2020 as these are now not directly comparable with current data. This is because the manner in which APP losses are identified and reported has changed, following the introduction of UK Finance Best Practice Standards in 2018 and the Contingent Reimbursement Model Code in 2019. In addition, the number of firms reporting APP data to us has increased.

All APP cases reported 2020-2021

	PERSONAL			NON PERSONAL			TOTAL		
	2020	2021	Change	2020	2021	Change	2020	2021	Change
Cases	145,207	188,964	**30%**	9,407	7,032	**-25%**	154,614	195,996	**27%**
Payments	228,946	333,751	**46%**	15,625	11,386	**-27%**	244,571	345,137	**41%**
Value	£347.4m	£505.9m	**46%**	£73.3m	£77.4m	**5%**	£420.7m	£583.2m	**39%**
Returned to Victim	£163.4m	£246.8m	**51%**	£27.4m	£24.4m	**-11%**	£190.8m	£271.2m	**42%**

- **Cases:** The number of confirmed cases reported, one case equals one account not one individual.
- **Payments:** Total number of payments identified as fraudulent in relation to case reported above.
- **Value:** The total value of payments reported above.
- **Returned to Victim:** The total amount returned to the victim either through a direct refund from the victim bank or through recovery of funds from the beneficiary account.

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.

Ten Payment Service Providers (PSPs), representing 19 consumer brands and over 90 per cent of authorised push payments, have signed up to the Code so far. A list of signatories can be found on the Lending Standards Board website.

In 2021, 182,976 cases were assessed and closed with a total value of £467.5 million. Our latest figures show that £238.1 million of losses were returned to victims under the APP voluntary code, accounting for 51 per cent of losses in these cases.

Reimbursement levels in 2021 were higher for more sophisticated scams in which criminals impersonate other organisations to target their victims. For police and bank impersonation scams, 61 per cent of all losses were refunded to the victim; the highest of all eight scam types.

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.

		< £1k	> £1k < £10k	> £10k	Total
Volume	Cases	127,473	47,040	8,463	182,976
	Payments	165,803	107,948	40,472	314,223
Value	Value	£37.8m	£148.7m	£281.0m	£467.5m
	Returned to Victim	£15.2m	£70.0m	£140.4m	£238.1m*

*This includes £12.4 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. However, 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:

- Collaborating with telecommunications and technology companies to stop fraud at source before victims lose money.
- Working with domain registries to prevent fraudulent and cloned websites.
- Sharing data with other sectors to stop fraud before it reaches the financial sector.
- 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 2021 the Unit prevented a record £101 million of fraud, the highest amount in its history, arrested 123 fraudsters, and secured 83 convictions. The unit also seized over £1.2 million of assets and disrupted 23 organised crime gangs.
- Collaborating with Pay.UK to improve data sharing within the payment journey to increase identification of fraudulent payments.
- 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. This took effect in March 2022.
- Introducing the industry-wide APP scams voluntary code, which helps to improve protections and reimburse many victims of these scams.
- Helping to prevent customers being duped by criminals by raising awareness of scams and how to stay safe through the Take Five 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 £202.8 million in fraud and led to 1,005 arrests since its launch in 2016.

Further analysis of the APP scam data

UK Finance collates 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 previous 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 APP voluntary code.

APP SCAM TYPES - PURCHASE SCAM

VALUE £64.1m + 25%

VOLUME 99,733 + 18%

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 2021, with the 99,733 cases accounting for 51 per cent of the total number of APP scam cases. A total of £64.1 million was lost to purchase scams in 2021, with the vast majority of losses being from personal accounts. Payment service providers were subsequently able to return £22.1 million of the losses.

Typically, purchase scams involve lower-value payments, with the smaller average case value meaning that they accounted for only 11 per cent of the total value of APP scams.

All purchase scam cases reported 2020-2021

	PERSONAL			NON PERSONAL			TOTAL		
	2020	2021	Change	2020	2021	Change	2020	2021	Change
Cases	80,214	97,382	21%	4,078	2,351	-42%	84,292	99,733	18%
Payments	102,325	129,442	27%	5,168	2,969	-43%	107,493	132,411	23%
Value	£44.7m	£56.8m	27%	£6.5m	£7.4m	13%	£51.1m	£64.1m	25%
Returned to Victim	£14.2m	£20.0m	41%	£1.7m	£2.1m	19%	£15.9m	£22.1m	39%

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.

		< £1k	> £1k < £10k	> £10k	Total
Volume	Cases	83,888	9,363	442	93,693
	Payments	104,761	21,480	1,378	127,619
Value	Value	£19.7m	£25.5m	£10.2m	£55.3m
	Returned to Victim	£7.0m	£8.3m	£3.5m	£18.8m

For those cases which were applicable for assessment using the voluntary code in 2021, 34 per cent of all losses were returned to the victim; the smallest proportion across all eight of the scam types.

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.

APP SCAM TYPES - INVESTMENT SCAM

VALUE	£171.7m	+ 57%

VOLUME	12,074	+ 48%

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 also seeking to take advantage of recent pension reforms.

Investment scam accounts for the largest proportion of losses of all eight APP scam types in 2021, a continuation of the trend seen in 2020 with losses of £171.7 million or 29 per cent of the overall total. The nature of the scams combined with the sophistication of the criminals mean that typically the sums involved in this type of scam are higher so while investment scam accounts for the largest proportion of loss, it only accounts for six per cent of the total number of APP scam cases.

Payment services providers were subsequently able to return £74.6 million to victims.

All investment scam cases reported 2020 - 2021

	PERSONAL			NON PERSONAL			TOTAL		
	2020	2021	Change	2020	2021	Change	2020	2021	Change
Cases	7,900	11,905	**51%**	281	169	**-40%**	8,181	12,074	**48%**
Payments	19,322	35,071	**82%**	601	594	**-1%**	19,923	35,665	**79%**
Value	£103.6m	£166.2m	**60%**	£5.8m	£5.5m	**-5%**	£109.4m	£171.7m	**57%**
Returned to Victim	£39.0m	£72.7m	**86%**	£1.2m	£2.0m	**66%**	£40.2m	£74.6m	**86%**

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.

		< £1k	> £1k < £10k	> £10k	Total
Volume	**Cases**	4,258	3,846	2,729	10,833
	Payments	6,903	10,498	11,961	29,362
Value	**Value**	£1.8m	£14.4m	£123.0m	£139.2m
	Returned to Victim	£0.6m	£4.5m	£57.3m	£62.4m

For only those cases which were applicable for assessment using the voluntary code, 45 per cent of all losses were returned to the victim in 2021.

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 Financial Conduct Authority (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 FCA'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.

APP SCAM TYPES - ROMANCE SCAM

VALUE	£30.9m	+ 73%

VOLUME	3,270	+ 41%

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 to start a relationship which they will try to develop over a longer period. 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 £30.9 million was lost to romance scams in 2021. With an average of nearly eight scam payments per case this was the highest of the eight scam types, highlighting evidence that the individual is often convinced to make multiple, generally smaller, payments to the criminal over a longer period.

Romance scams accounted for less than two per cent of the total number of APP scam cases in 2021 and only five per cent of the total value. Payment service providers were only able to return £12.6 millions (41%) of the losses, often due to the fact that the payments were made over an extended period meaning the money had been moved by the criminal by the time the scam was reported.

All romance scam cases reported 2020-2021

	PERSONAL			NON PERSONAL			TOTAL		
	2020	2021	Change	2020	2021	Change	2020	2021	Change
Cases	2,252	3,245	**44%**	73	25	**-66%**	2,325	3,270	**41%**
Payments	12,778	25,723	**101%**	407	91	**-78%**	13,185	25,814	**96%**
Value	£17.3m	£30.6m	**77%**	£0.5m	£0.3m	**-41%**	£17.8m	£30.9m	**73%**
Returned to Victim	£6.5m	£12.4m	**91%**	£0.1m	£0.2m	**109%**	£6.6m	£12.6m	**92%**

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.

		< £1k	> £1k < £10k	> £10k	Total
Volume	**Cases**	1,998	1,282	527	3,807
	Payments	3,787	10,177	9,483	23,447
Value	**Value**	£0.5m	£4.7m	£20.5m	£25.7m
	Returned to Victim	£0.2m	£2.0m	£9.1m	£11.3m

For only those cases which were applicable for assessment using the voluntary code, 44 per cent of all losses were returned to the victim in 2021.

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.
- 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.

APP SCAM TYPES - ADVANCE FEE SCAM

VALUE	**£32.1m**	**+ 45%**	**VOLUME**	**20,495**	**+ 48%**

In an advance fee scam, a criminal convinces their victim to pay a fee which they claim will 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 2021, accounting for ten per cent of the total number of cases. A total of £32.1 million was lost to advance fee scams last year, nearly six per cent of all APP scams.

All advance fee scam cases reported 2020 - 2021

	PERSONAL			NON PERSONAL			TOTAL		
	2020	2021	Change	2020	2021	Change	2020	2021	Change
Cases	13,316	19,950	**50%**	517	545	**5%**	13,833	20,495	**48%**
Payments	22,434	36,166	**61%**	798	804	**1%**	23,232	36,970	**59%**
Value	£21.2m	£30.8m	**45%**	£1.0m	£1.4m	**34%**	£22.2m	£32.1m	**45%**
Returned to Victim	£7.4m	£10.9m	**48%**	£0.3m	£0.9m	**194%**	£7.7m	£11.8m	**53%**

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 scam cases reported and should not be treated as an addition.

		< £1k	> £1k < £10k	> £10k	Total
Volume	**Cases**	16,386	3,651	422	20,459
	Payments	23,124	8,503	2,565	34,192
Value	**Value**	£4.9m	£9.1m	£13.3m	£27.2m
	Returned to Victim	£2.1m	£2.8m	£4.4m	£9.3m

For only those cases which were applicable for assessment using the voluntary code, 34 per cent of all losses were returned to the victim in 2021.

How to stay safe from advance fee scams:

- Question claims that you are 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 i.e. 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 victim to an advance fee scam.

APP SCAM TYPES - INVOICE AND MANDATE SCAMS

VALUE	£56.7m	- 17%	VOLUME	4,330	- 8%

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 2021, however they accounted for ten per cent of all APP losses, totalling £56.7 million. Most losses occurred on a non-personal or business account, some £36.8 million, where the average payment was more than £14,000. This reflects the fact that businesses make genuine higher-value payments more regularly, making it harder to spot and stop a fraudulent one.

All invoice and mandate scam cases reported 2020 – 2021

	PERSONAL			NON-PERSONAL			TOTAL		
	2020	2021	Change	2020	2021	Change	2020	2021	Change
Cases	2,903	2,555	**-12%**	1,818	1,775	**-2%**	4,721	4,330	**-8%**
Payments	3,904	3,676	**-6%**	2,416	2,491	**3%**	6,320	6,167	**-2%**
Value	£25.1m	£19.9m	**-21%**	£43.6m	£36.8m	**-16%**	£68.8m	£56.7m	**-17%**
Returned to Victim	£15.7m	£12.6m	**-20%**	£16.1m	£10.2m	**-37%**	£31.8m	£22.8m	**-28%**

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 scam cases reported and should not be treated as an addition.

		< £1k	> £1k < £10k	> £10k	Total
Volume	**Cases**	966	1,774	525	3,265
	Payments	1,166	2,370	931	4,467
Value	**Value**	£0.4m	£6.2m	£20.4m	£27.0m
	Returned to Victim	£0.2m	£3.2m	£12.8m	£16.2m

For only those cases which were applicable for assessment using the voluntary code, 61 per cent of all losses were returned to the victim.

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.

APP SCAM TYPES - CEO FRAUD

VALUE	**£12.7m**	**+ 165%**	**VOLUME**	**461**	**+ 29%**

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 2021, accounting for less than one per cent of total cases. A total of £12.7 million was lost, equivalent to two per cent of the total case value.

	PERSONAL			NON-PERSONAL			TOTAL		
	2020	**2021**	**Change**	**2020**	**2021**	**Change**	**2020**	**2021**	**Change**
Cases	82	65	**-21%**	275	396	**44%**	357	461	**29%**
Payments	127	99	**-22%**	360	579	**61%**	487	678	**39%**
Value	£0.9m	£1.1m	**27%**	£3.9m	£11.6m	**196%**	£4.8m	£12.7m	**165%**
Returned to Victim	£0.5m	£0.7m	**33%**	£1.5m	£2.4m	**61%**	£2.0m	£3.1m	**54%**

Only those cases assessed using the voluntary code by signatory PSPs

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

		< £1k	**> £1k < £10k**	**> £10k**	**Total**
Volume	**Cases**	23	114	81	218
	Payments	33	144	168	345
Value	**Value**	£0.0m	£0.7m	£2.9m	£3.6m
	Returned to Victim	£0.0m	£0.4m	£1.7m	£2.1m

For only those cases which were applicable for assessment using the voluntary code, 57 per cent of all losses were returned to the victim.

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

APP SCAM TYPES - IMPERSONATION: POLICE/BANK STAFF

VALUE	£137.3m	+ 51%

VOLUME	29,406	+ 39%

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 15 per cent of all APP scam cases in 2020. £137.3 million was lost due to these scams, which by value was the second highest type of APP scam, accounting for 24 per cent of total losses. Payment service providers were able to return £84.8 million of the losses to customers.

	PERSONAL			NON PERSONAL			TOTAL		
	2020	2021	Change	2020	2021	Change	2020	2021	Change
Cases	20,199	28,629	**42%**	978	777	**-21%**	21,177	29,406	**39%**
Payments	37,232	60,931	**64%**	3,365	1,875	**-44%**	40,597	62,806	**55%**
Value	£84.3m	£130.3m	**55%**	£6.6m	£7.0m	**7%**	£90.9m	£137.3m	**51%**
Returned to Victim	£53.9m	£80.7m	**50%**	£4.2m	£4.1m	**-2%**	£58.0m	£84.8m	**46%**

Only those cases assessed using the voluntary code by signatory PSPs

All cases reported below are also included in previous figures relating to all Impersonation: Police/Bank staff scam cases reported and should not be treated as an addition.

		< £1k	> £1k < £10k	> £10k	Total
Volume	**Cases**	8,221	16,848	2,679	27,748
	Payments	11,291	36,719	9,897	57,907
Value	**Value**	£4.6m	£58.4m	£60.8m	£123.8m
	Returned to Victim	£2.6m	£35.6m	£37.8m	£76.1m

For only those cases which were applicable for assessment using the voluntary code, 60 per cent of all losses were returned to the victim; the highest of all eight scam types.

How to stay safe from 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 or full password.
- 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.
- 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.

APP SCAM TYPES - IMPERSONATION: OTHER

VALUE	£77.5m	+ 39%

VOLUME	26,227	+ 33%

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 £77.5 million was lost to this type of scam in 2021, with payment service providers subsequently able to return £39.4 million. Impersonation: other accounted for 13 per cent of all APP scam cases last year and also 13 per cent of total losses.

	PERSONAL			NON PERSONAL			TOTAL		
	2020	2021	Change	2020	2021	Change	2020	2021	Change
Cases	18,341	25,233	**38%**	1,387	994	**-28%**	19,728	26,227	**33%**
Payments	30,824	42,643	**38%**	2,510	1,983	**-21%**	33,334	44,626	**34%**
Value	£50.4m	£70.1m	**39%**	£5.4m	£7.4m	**37%**	£55.8m	£77.5m	**39%**
Returned to Victim	£26.2m	£36.8m	**40%**	£2.3m	£2.6m	**11%**	£28.6m	£39.4m	**38%**

Only those cases assessed using the voluntary code by signatory PSPs

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

		< £1k	> £1k < £10k	> £10k	Total
Volume	**Cases**	11,733	10,162	1,058	22,953
	Payments	14,738	18,057	4,089	36,884
Value	**Value**	£6.1m	£29.7m	£29.9m	£65.6m
	Returned to Victim	£2.4m	£13.3m	£13.8m	£29.6m

For only those cases which were applicable for assessment using the voluntary code, 45 per cent of all losses were returned to the victim.

How to stay safe from other impersonation scams:

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

PAYMENT TYPE

This data shows the type of payment method the victim used to make the payment in the authorised push payment scam. Faster Payments was used for 97 per cent of fraudulent APP scam payments. While CHAPS was the least common payment method, representing only 0.2 per cent of cases, the high-value nature of transactions using this payment type meant that it accounted for four per cent of the total value.

	Number of Payments			Value		
Payment Type	**2020**	**2021**	**Change**	**2020**	**2021**	**Change**
Faster Payment	236,641	335,451	**42%**	£349.4m	£504.5m	**44%**
CHAPS	501	764	**52%**	£14.5m	£22.5m	**55%**
BACs	1,193	1,695	**42%**	£23.5m	£20.4m	**-13%**
Intra Bank Transfer ("on us")	3,113	3,358	**8%**	£10.6m	£7.5m	**-29%**
International	3,123	3,869	**24%**	£22.7m	£28.3m	**25%**
Total	**244,571**	**345,137**	**41%**	**£420.7m**	**£583.2m**	**39%**

PAYMENT CHANNEL

This data shows the channel through which the victim made the authorised push payment. The most common payment channel was mobile banking which accounted for 58 per cent of the payment volume but only 30 per cent of the loss, indicating the typically lower payment limits available to customers within the mobile banking channel.

	Number of Payments			Value		
Payment Type	**2020**	**2021**	**Change**	**2020**	**2021**	**Change**
Branch	8,968	8,251	**-8%**	£43.6m	£56.6m	**30%**
Internet Banking	113,853	130,016	**14%**	£262.5m	£329.1m	**25%**
Telephone Banking	5,593	6,249	**12%**	£17.8m	£24.4m	**37%**
Mobile Banking	116,157	200,621	**73%**	£96.9m	£173.2m	**79%**
Total	**244,571**	**345,137**	**41%**	**£420.7m**	**£583.2m**	**39%**

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.

35 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: and the police. They spend hours researching you 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 the campaign visit: http://www.takefive-stopfraud.org.uk

LIST OF MEMBERS WHO HAVE CONTRIBUTED DATA TO THIS PUBLICATION

- Allied Irish Bank
- American Express
- Bank of Ireland
- Barclays Bank
- C Hoare & Co
- Capital One
- Citibank
- Co-Operative Financial Services
- Coventry Building Society
- Danske Bank
- Hampden & Co
- HSBC
- Investec
- Lloyds Banking Group
- Marks & Spencer
- Metro Bank
- Modulr
- Nationwide
- New Day
- Royal Bank of Scotland Group
- Sainsburys Bank
- Santander
- Secure Trust Bank
- Silicon Valley Bank
- Starling Bank
- Tesco Bank
- Triodos Bank
- TSB
- Vanquis
- Virgin Money
- Weatherbys Bank
- Yorkshire Bank
- Zopa Bank

METHODOLOGY FOR DATA COLLECTION

All our data is collected directly from the firms we represent. We do not make any estimations (unless indicated) and have agreed definitions/reporting templates in use to ensure consistency across firms. All data submitted must pass three clear plausibility phases (below) before publication.

Validation check

Datasets containing totals, sub-totals, less-than or non-nil data field rules are automatically checked by the system, highlighting erroneous data content. Such errors result in a 'failed submission' which requires amendment.

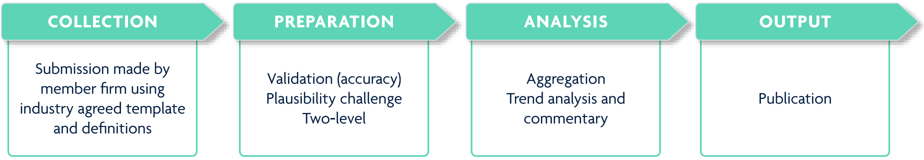
Data plausibility – outputs

For high priority, public-facing data series, data management spreadsheets incorporate visible warnings if a data observation is a series outlier or falls outside defined tolerance intervals.

Data plausibility - inputs

Arithmetically correct data for individual members is subject to rangecheck scrutiny against previously submitted data (automated within spreadsheets or by manual assessment) at a granular component level. Further challenge is undertaken, if possible, by (explicit or implicit) reference to alternative relevant data sources submitted by that member firm. Such subjective challenges are raised to subject matter experts and resolved with data providers.

A typical process for one submission from one member would look like the below.



Without evidence of the above, data will not be published.

Disclaimer

This report is intended to provide information only and is not intended to provide financial or other advice to any person. While all reasonable efforts have been made to ensure the information contained above was correct at the time of publication, no representation or undertaking is made as to the accuracy, completeness or reliability of this report or the information or views contained in this report. None of UK Finance or its employees or agents shall have any liability to any person for decisions or actions taken based on the content of this document.