



UK FINANCE

ANNUAL FRAUD REPORT

The definitive overview of
payment industry fraud in 2022



Sponsored by:



UK Finance is the collective voice for the banking and finance industry. Representing more than 300 firms across the industry, it seeks to enhance competitiveness, support customers and facilitate innovation.

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

UK Finance seeks to ensure that the UK is the safest and most transparent financial centre in the world – 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	1	REMOTE BANKING FRAUD	37
INTRODUCTION	2	Unauthorised remote banking fraud	38
UK Finance	2	Internet banking fraud	40
Foreword from Feedzai	4	Telephone banking fraud	42
		Mobile banking fraud	44
TRENDS AND STATISTICS	6	AUTHORISED FRAUD	46
2022 Overview	7	Authorised push payment (APP) fraud	47
Behind the changing fraud figures	7	Fraud origination	49
The industry response	9	APP voluntary code	51
Technology	11	Further analysis of the APP scam data	52
CARD FRAUD	12	APP SCAM TYPES	53
Unauthorised debit, credit and other payment card fraud	13	Purchase scam	53
Card fraud volumes	15	Investment scam	55
Remote purchase (Card-not-present) fraud	17	Romance scam	57
Counterfeit card fraud	19	Advance fee scam	59
Lost and stolen card fraud	21	Invoice and mandate scam	61
Card ID theft	23	CEO scam	63
Card not received fraud	26	Impersonation: police/bank staff scam	65
		Impersonation Scam: Other	67
FURTHER CARD FRAUD ANALYSIS	28	Payment type	69
UK retail face-to-face card fraud losses	28	Payment channel	69
Internet/E-commerce fraud	30	TAKE FIVE TO STOP FRAUD	70
Card fraud at UK cash machines	31	CONTRIBUTING MEMBERS	71
Card fraud abroad	32	METHODOLOGY FOR DATA COLLECTION	72
CHEQUE FRAUD	34	APPENDIX	73
Unauthorised cheque fraud	35	Cases	73
		Gross losses	73

OUR FRAUD DATA

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

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

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

Some caveats apply to 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

The banking industry spends billions of pounds each year fighting fraud, but criminals continue to commit this crime and losses exceeded £1 billion for another year running. That is equivalent to around £2,300 stolen every minute of last year.

In all its forms, fraud accounts for over 40 per cent of crimes committed in England and Wales.

This is the scale of the problem we face and the banking and finance sector is at the forefront of efforts to tackle fraud. We still need much greater action from other sectors as criminals are clearly exploiting weaknesses outside the banking system.

The government's recent fraud strategy rightly says we need to focus on stopping fraud at source and that "it is other industries, especially online technology giants, who should do more to stop criminals exploiting their services."

The need for other sectors to act is shown by our analysis of thousands of authorised push payment (APP) fraud cases. We found that 78 per cent of APP fraud starts online and another 18 per cent via telecoms.

This year's figures

This year's report shows that over £1.2 billion was stolen through fraud in 2022, a reduction of eight per cent compared to 2021. Within that overall figure, unauthorised fraud losses were £726.9 million (down less than one per cent) and APP fraud losses were £485.2 million (down 17 per cent). Protections such as Strong Customer Authentication (SCA) and

Confirmation of Payee are having an impact, but too much money is still getting into the hands of criminals.

It is not just the money lost that is devastating to victims. There are huge emotional and psychological impacts on people.

The ongoing cost of living challenge has seen criminals take advantage of people's anxieties around their finances. This includes fake investment opportunities, cheap deals which turn out to be purchase scams, and impersonation fraud that tricks people into handing over personal details and passwords which are then used to access financial accounts or set up fake ones.

More can be done to prevent fraud, including easier data-sharing, increased law enforcement capacity, collaboration with other sectors and greater powers for firms to use funds that are proceeds of crime.

Legislative changes

There are important and welcome legislative changes taking place, in which we have been actively involved.

The preventative fraud measures in the Online Safety Bill will for the first time mean that technology and social media companies will have to remove scam adverts from their platforms. Online platforms and telcos need to work harder at closing down the opportunities for fraudsters to use their systems.

The **Economic Crime and Corporate Transparency Bill** has key provisions on reform of Companies House and tackling money

laundering, as well as helping with information sharing and the seizure of crypto assets.

The Payment Systems Regulator is consulting on an approach to fraud reimbursement. This will replace the APP voluntary code which has already seen the industry reimburse hundreds of millions of pounds to fraud victims. Reimbursement rates have increased again this year, but relying on the banking sector alone to reimburse victims of fraud means the platforms that facilitate the majority of the fraud have no financial incentive to stop it. And at the end of the day, the criminal still gets away with victims' money.

Alongside these, the changes that the government is looking to make to enable a risk-based approach to payments, giving firms additional time to investigate certain suspicious transactions is a welcome change we have been calling for.

Partnerships

Our partnerships with the private sector, law enforcement, regulators and government remain critical. In 2022 the **Dedicated Card and Payment Crime Unit (DCPCU)**, a specialist police unit funded by the banking and finance industry, celebrated its 20th year

of investigating and targeting the organised criminal gangs behind payment crime. In its time it has convicted over 1,000 criminals. Last year it worked closely with the Metropolitan Police on **Operation Elaborate**, an operation to shut down a website that was openly selling services to help people commit fraud. This was intelligence-led policing to target criminal gangs proactively, disrupting them at source, rather than trying to deal with the aftermath.

Finally, UK Finance and its members have continued to raise consumer awareness through the **Take Five to Stop Fraud** campaign, which provides straight-forward advice to help people stay safe.

Plenty of challenges remain. Criminal gangs – well-organised, tech-savvy and merciless – are adept at changing tactics. That is why we all need to work together to fight fraud as it remains a persistent threat to businesses, consumers and the growth of the economy, not to mention the reputation of the UK as a place to do business.

David Postings,

Chief Executive of UK Finance

FOREWORD FROM FEEDZAI

Feedzai, the world's first RiskOps platform, is proud to collaborate with UK Finance for the 2023 Annual Fraud Report. As a trusted partner to several UK banks, we're delighted to have this opportunity to share our experience and to reflect on the bare facts of UK fraud in 2022.¹

2022 was the year that consumers hoped they could finally put the Covid-19 pandemic behind them and return to some form of normality. However, this hope didn't last long as the global macro-economic impacts of the war in Ukraine contributed to already strained global supply chain issues and exacerbated the UK's cost of living crisis.

The combination of economic change with ever-increasing sophistication from fraudsters has again changed the risk landscape. With many consumers feeling financially vulnerable, fraud problems such as money muling are poised to increase. In fact, Feedzai's survey revealed that 37 per cent of respondents had been approached on social media to either receive funds into their accounts or to share their account details. Furthermore, despite renewed focus by the banks, a third of respondents were unaware of the potentially life-changing consequences of processing fraudulent funds on behalf of a third party.

Scams, in particular, have become so prominent that the UK has become the world leader in detection, sophistication, customer education and victim reimbursement policy. This trend is largely attributed to investment by banks and the subsequent success in preventing unauthorised fraud. By putting up such strong defence mechanisms, banks have forced fraudsters to target the customer as the weakest part of the decision chain.

These scams now take a multitude of forms, including romance, investment, purchase, and impersonation scams, to name just a few. Despite this, advancements in technology, and in particular the use of AI to enhance fraud decisioning, have enabled the banks to make positive steps forward in 2022. Although UK Finance data shows a six per cent increase in scam cases, losses were down by 17 per cent, demonstrating that persistent focus is starting to pay off as the average loss per case was significantly reduced.

One thought to consider however, is that it is not just the banks that are utilising AI technology. Fraudsters are already starting to adopt AI to amplify their attack sophistication, with the use of generative AI like ChatGPT and voice cloning poised to make scams ever more convincing. Meanwhile, the role of **Big Tech in connecting scammers** with victims is also drawing scrutiny.

The UK is not alone in this problem though. According to the **FTC in the US**, consumers reported losing more than £3 billion to investment scams in 2022. That amount more than doubles the amount reported lost in 2021. In Australia over £300 million **was lost to scams in 2022**. Over half that amount was from investment scams, followed by romance scams.

¹ Feedzai. "The Human Impact of Fraud and Financial Crime on Customer Trust" April 18, 2023. <https://feedzai.com/resource/the-human-impact-of-fraud-and-financial-crime-on-customer-trust-in-banks/>

The data collated by UK Finance for this report shows that in 2022 overall Authorised Push Payment (APP) reimbursement rates exceeded 50 per cent for the first time, at an average across all typologies of 59 per cent. Nevertheless, the UK's Payment Systems Regulator (PSR) has proposed a series of measures designed to enhance consumer protection even further. The proposal being discussed aims to create additional financial protection for victims, with a liability split between the sending and receiving institutions – a world first. Additionally, the PSR plans include publicly sharing data on how frequently each bank refunds a victim.

The impacts of these proposals will be huge as consumers, for the first time, will see how well their bank is handling scam risks. Banks that perform badly in this peer-to-peer comparison may well see customers take their banking relationship elsewhere; those that perform well on the other hand may be more attractive to consumers due to a perceived higher rate of security. Meanwhile, the possible shift in liability from sending bank to receiving bank will place a revised emphasis on mule account detection. This will drive fraud and anti-money laundering (AML) teams to collaborate more closely than ever before.


Globally, the world's eyes will be firmly fixed on the UK approach. Pressure is mounting as each region plans its own respective regulatory response.

While scams receive the lion's share of attention, UK Finance data reveals that unauthorised fraud is still a significant concern. Despite a decrease of one per cent, losses totalled £726.9 million with almost three million cases recorded. Some key trends saw losses related to lost and stolen cards increase by 30 per cent, contactless payment fraud by 82 per cent, and in-person card transactions by 34 per cent. Remote purchase (CNP) fraud still contributes the majority of unauthorised losses with £395.7 million reported. With PSD2 Strong Customer Authentication (SCA) regulation being implemented by the industry on 14th March 2022, 2023 may well provide some insight into how effective this regulation has been.

With fraud sophistication growing across all channels, banks must continue to focus on a customer-centric approach to fraud detection. Putting the customer at the heart of the risk decision and creating a channel-agnostic view of all available data is the most effective way to recognise risk and keep customers safe. Feedzai is proud to support UK Finance's efforts to raise awareness of these key industry threats and help UK banks in their ongoing efforts to make banking and commerce safer for their customers.

Dan Holmes

Fraud Prevention Strategy
& Subject Matter Expert, Feedzai



+11,00.00

TRENDS AND STATISTICS

2022 OVERVIEW

Overall fraud losses (both authorised and unauthorised) totalled £1.2 billion in 2022; a decrease of eight per cent when compared to 2021. UK Finance members reported 2,988,705 cases of confirmed fraud, a reduction of four per cent in the same period.

Unauthorised financial fraud losses across payment cards, remote banking and cheques totalled £726.9 million in 2022, a decrease of less than one per cent. Banks and card companies prevented £1.2 billion in unauthorised fraud in 2022. This represents incidents that were detected and prevented by firms and is equivalent to 61.5p in every £1 of attempted fraud being stopped. In addition to this, there were 207,372 incidents of authorised push payment (APP) scams reported in 2022 with gross losses of £485.2 million, compared with £583.2 million in 2021.

BEHIND THE CHANGING FRAUD FIGURES

The end of the pandemic has reshaped the fraud landscape in the past 12 months, resulting in certain types of fraud falling while others have risen. Criminals continue to focus on methods 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. This can occur on a multitude of platforms such as social media, auction sites and search engines.

Intelligence reported by our members highlights some of 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 2022. Typically, the fraud types that have seen an increase in losses are those that require the theft of significant amounts of personal information, such as card ID theft. Criminals focus attempts on socially

engineering personal information from their victims with a view to committing authorised push payment (APP) fraud in which the victim makes the payment themselves. If this is not successful, the criminal often has enough personal information to enable them instead to impersonate their victims, with a view to either taking control of their existing accounts or applying for credit cards in their name.

Certain types of APP fraud that involve socially engineering the victim in one way or another have increased. Criminals are using tactics such as scam phone calls, text messages and emails, as well as fake websites and social media posts, to trick people into handing over personal details and passwords. This information is then used to target victims and convince them to authorise payments. For the first time UK Finance has published data relating to the origination of authorised push payment cases

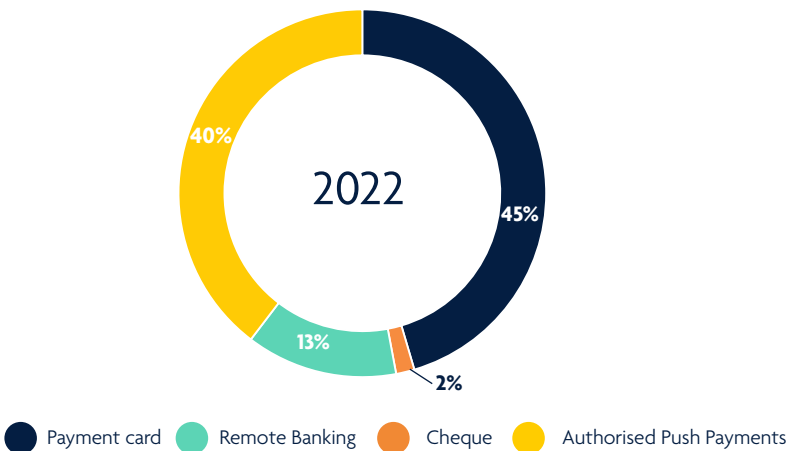
which shows that 78% of authorised push payment fraud started online during H2 2022.

With the ever-evolving landscape in the way criminals operate, industry has also had to adapt methods to prevent frauds from happening in the first place. This has resulted in frauds now being prevented much earlier in the payment journey. Confirmation of Payee, effective warning messages tailored to the payment type during the payment journey, and general education and awareness campaigns (such as UK Finance's **Take Five to Stop Fraud**) mean that banks have been able to prevent frauds occurring before a fraudulent transaction takes place. This explains why prevented fraud appears to have decreased in 2022. The attack level has remained consistent with previous years, but fraud is being prevented earlier and so is more difficult to capture and record.

Smishing and phishing attacks took advantage of people's need to access online services rather than in person, often targeting smaller amounts (delivery fees etc) with the intention of stealing the victims information to then commit further fraud. While customers of all age groups are falling victim to these scams, it is younger age groups that are often the prime target. Research suggests 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 2022 financial fraud losses by type % of total



THE INDUSTRY RESPONSE

The banking and finance industry is working hard to protect customers from fraud, including partnering with other sectors, government and law enforcement to prevent and disrupt this criminal activity and bring fraudsters to justice. The industry is responding to this threat by:

1. Launching a new Industry Fraud and Scams Strategy in 2022 which is focused on stopping fraud at source and working with all stakeholders involved to collaborate to close vulnerabilities in each part of the fraud journey. The strategy focuses on:
 - Upstream collaboration with telcos and tech firms
 - Intelligence sharing within financial services and cross-sector
 - Specific actions through the payment journey to identify fraud in real time
 - Customer empowerment and protection
2. Working with the government and regulators to ensure the legislative framework supports a robust response to fraud. We have been engaging with government and parliamentarians to ensure progression of robust legislation most recently in relation to the Online Safety Bill, Financial Services and Markets Bill and Economic Crime and Corporate Transparency Bill.
3. Working with government on the recently published second Economic Crime Plan ('the Plan'). The Plan is outcomes-focused and reflects a shared focus on directing public-private resource towards agreed priorities to maximise collective action against the threat of economic crime.

For the first time, fraud was included within the scope of the Plan with one of the outcomes being to cut fraud against individuals and businesses.
4. Engaging with the government on its new Fraud Strategy.
5. Engagement and attendance at the Joint Fraud Task Force and Online Fraud Group and delivery of commitments contained in the Retail Banking Fraud Charter.
6. 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.
7. 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 2022, 2.96 million compromised card numbers were received through law enforcement and disseminated by the I&I Unit to enable card issuers to take the necessary precautions to protect customers.
 - It is hoped that the new information sharing provisions within the Economic Crime and Corporate Transparency Bill will better enable the regulated sector

to share information across a wide spectrum of economic crime, further strengthening the industry's ability to identify and mitigate threats.

8. Delivering customer education campaigns to help individuals stay safe from fraud, spot the signs of a scam, and prevent consumers being duped by criminals. These include our Take Five to Stop Fraud and Don't Be Fooled campaigns. 38 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 employees to spot and stop suspicious transactions. The Banking Protocol rapid response scheme allows 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.
9. In 2022 a three-year funding stream was secured to enable the Dedicated Card and Payment Crime Unit (DCPCU) to build a team to tackle emerging crypto cyber enabled threats. This new team helped the unit achieve industry savings of £41 million in 2022 alone.
10. Continuing to work with the regulator Ofcom to crack down on number spoofing through the 'do not originate' list. This work has resulted in ongoing protection for financial institutions as criminals are prevented from spoofing the phone numbers of trusted organisations including the numbers on the back of bank cards.
11. Working with text message providers and law enforcement to block scam text messages. 3017 unauthorised sender IDs are currently being blocked to prevent them being used to send scam text messages mimicking trusted organisations.
12. Working collaboratively with **Pay.UK** on a design solution for additional data points to be shared by sending and receiving firms when payments are being generated to enable real-time identification of fraud.

TECHNOLOGY

- The banking industry continues to make proactive use of technology in the fight against fraud.
- One example is the use of a system – 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, banks 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.
- UK Finance works closely on cross sector collaboration with telecommunications and technology stakeholders to assess and close down vulnerabilities across the wider ecosystem, including upstream in the customer journey. The Industry Fraud and Scams Strategy is focused on working on technical developments to enable Payment Service Providers to manage risk more effectively.
- Collaboration between the banking and telecoms sector continues to evolve with new data sharing exercises which increase the detection of high-risk phone calls. This is now in the process of being rolled out across all mobile networks in a phased manner. To combat telephone banking fraud, some banks are using technology to profile the risks associated with calls based on a combination of network authentication, audio modulation and AI technologies. 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.
- A recently concluded collaboration with an online platform showed there is immense potential for real time intelligence exchange between sectors to identify and stop advertising fraud at source. Replication of this is being explored across additional platforms.
- Finally, the industry is engaging strategically with the investment industry to enhance investment protocols and share data effectively to help mitigate bad actors impersonating genuine firms.



CARD FRAUD

UNAUTHORISED DEBIT, CREDIT AND OTHER PAYMENT CARD FRAUD

VALUE **£556.3m**

+ 6%

VOLUME **2,732,894**

- 3%

Fraud losses on UK-issued cards totalled £556.3 million in 2022, a six per cent rise from £524.5 million in 2021. At the same time, total spending on all debit and credit reached nearly £1 trillion in 2022, with 28 billion transactions made during the year.

Overall card fraud losses as a proportion of the amount we spend on our cards decreased during 2022, falling from 6.3 pence per £100 spent in 2021 to six pence per £100 in 2022.

A total of £967 million in card fraud was stopped by banks and card companies in 2022, the same amount as in 2021. This is equivalent to £6.35 in every £10 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 (also known as 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. Strong customer authentication for higher value online payments was implemented by the industry on 14 March 2022, adding an extra layer of security in the fight against fraud.
- Industry implementation of PSD2 Strong Customer Authentication (SCA) regulation. Speedily, safely, and securely identifying compromised card details through UK Finance's intelligence hub so that card issuers can put protections in place.
- 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 2022 the unit prevented an estimated £41 million of fraud and arrested 141 suspected fraudsters.

Card Fraud Losses 2013 - 2022

Fraud Type	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	% Change 21/22
Remote Purchase (CNP)	£301.0m	£331.5m	£398.4m	£432.3m	£408.4m	£506.4m	£470.2m	£452.6m	£412.5m	£395.7m	-4%
Of which -commerce	£190.1m	£219.1m	£261.5m	£310.3m	£310.4m	£394.2m	£360.5m	£376.5m	£338.9m	£285.2m	-16%
Counterfeit	£43.3m	£47.8m	£45.7m	£36.9m	£24.2m	£16.3m	£12.8m	£8.7m	£4.7m	£4.7m	1%
Lost and Stolen	£58.9m	£59.7m	£74.1m	£96.3m	£92.9m	£95.1m	£94.8m	£78.9m	£77.2m	£100.2m	30%
Card ID Theft	£36.7m	£30.0m	£38.2m	£40.0m	£29.8m	£47.3m	£37.7m	£29.7m	£26.3m	£51.7m	97%
Card non-receipt	£10.4m	£10.1m	£11.7m	£12.5m	£10.2m	£6.3m	£5.2m	£4.4m	£3.9m	£4.0m	1%
Total	£450.2m	£479.0m	£568.1m	£618.1m	£565.4m	£671.4m	£620.6m	£574.2m	£524.5m	£556.3m	6%
UK	£328.2m	£328.7m	£379.7m	£417.9m	£407.5m	£496.6m	£449.9m	£414.5m	£384.0m	£417.0m	9%
Fraud Abroad	£122.0m	£150.3m	£188.4m	£200.1m	£158.0m	£174.8m	£170.7m	£159.7m	£140.5m	£139.3m	-1%

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 (2.73million) reported during 2022 fell by three per cent in comparison to the number reported in 2021 (2.82million).

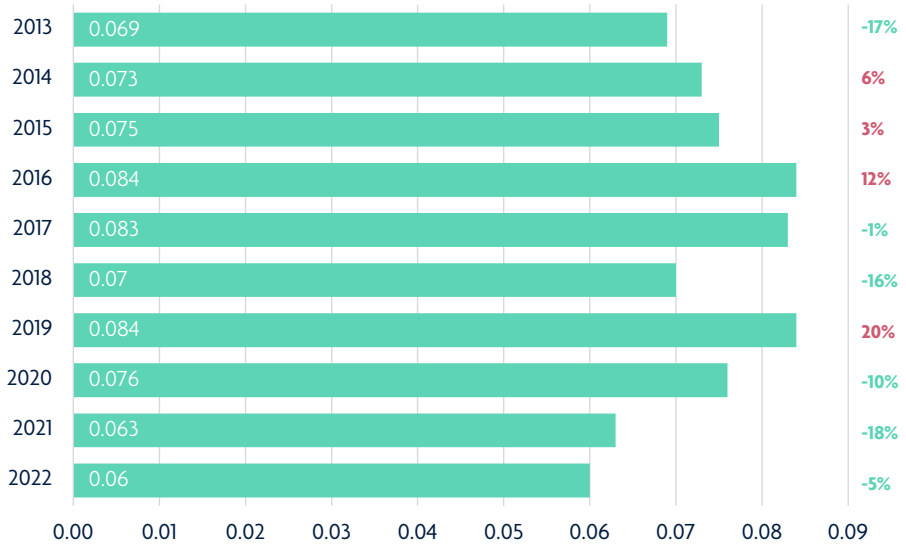
Remote purchase (CNP) accounts for the biggest proportion of card fraud with 81 per cent of all card fraud cases reported involving the use of stolen card details to buy something on the internet, over the phone or through mail order.

Cases of counterfeit cards have fallen to the lowest ever levels reported due to the success of Chip and PIN.

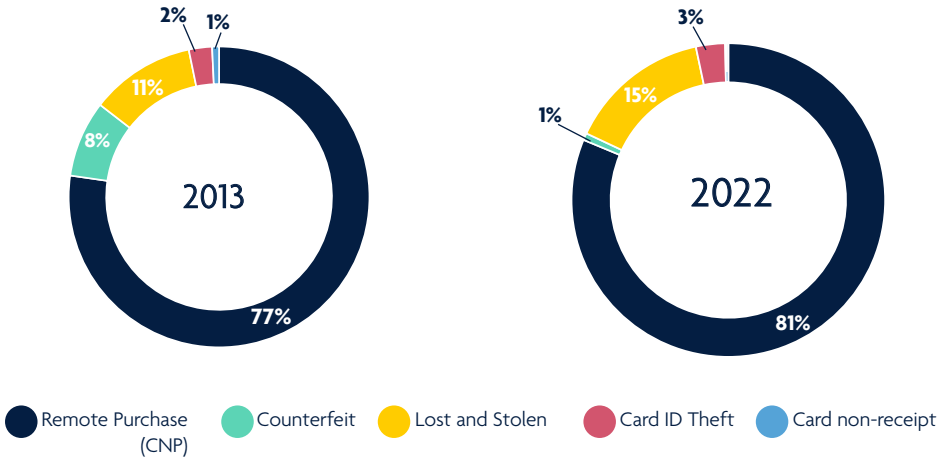
It is important to note that the number of cases relates to the number of accounts that have been defrauded, as opposed to the number of victims.

	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	% Change 21/22
Remote Purchase (CNP)	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	2,221,045	-8%
Counterfeit	101,109	99,279	86,021	108,597	85,025	58,636	65,907	52,782	24,908	19,594	-21%
Lost and Stolen	138,967	133,943	143,802	231,164	350,279	434,991	460,142	321,994	325,501	401,343	23%
Card ID Theft	30,718	26,542	33,566	31,756	29,156	63,791	54,165	34,545	40,026	82,064	105%
Card non-receipt	9,125	9,302	10,719	11,377	10,903	10,046	7,907	8,435	8,941	8,848	-1%
	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	2,732,894	-3%

Fraud to turnover ratio 2013-2022



Card fraud losses 2022 split by type (as a percentage of total losses)



REMOTE PURCHASE (CARD-NOT-PRESENT) FRAUD

VALUE **£395.7m** **- 4%**

VOLUME **2,221,045** **- 8%**

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 £395.7 million in 2022, a decrease of four per cent when compared with 2021 and the first-time losses have fallen below £400 million since 2015. Online fraud against UK retailers totalled an estimated £295 million in 2022, a decrease of three per cent from £303 million on the previous year.

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.

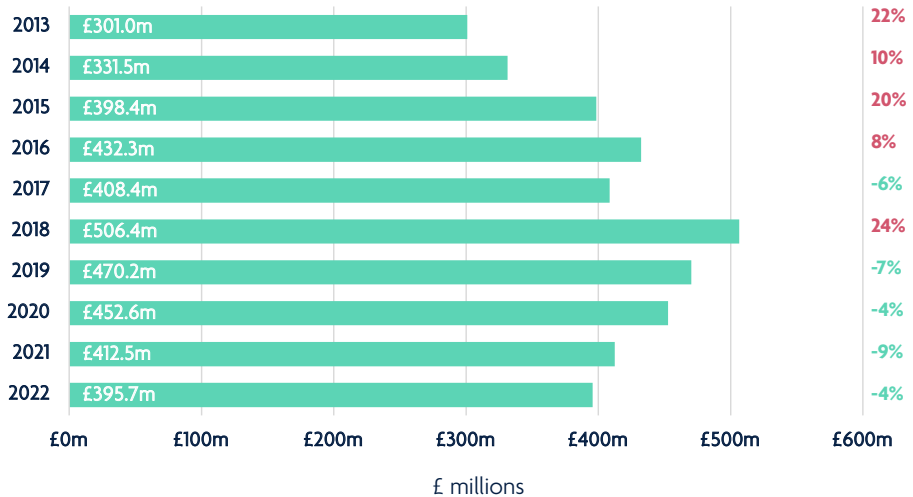
"Digital skimming" is another method criminals use to steal card data from customers when they shop online. In a typical digital skimming attack, criminals will add malicious code to the online retailer's website which steals sensitive information including card details at the check-out stage. This information 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) to e-commerce took effect. This follows the managed programme which UK Finance led on behalf of members 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. To circumvent these additional protections, criminals are increasingly using social engineering techniques to trick customers into divulging their one-time passcodes (OTPs) so they can authenticate fraudulent online card transactions. In some cases, customers are also being tricked by criminals into making online card transactions themselves.

One-time passcodes (OTPs) should be treated in the same way as a PIN in that they should never be shared with anyone, including a bank. Before entering a OTP, customers must check it accurately describes the transaction or purchase they are about to make. If codes are received unexpectedly, customers should contact their bank immediately on a number known to be correct, such as the one listed on the back of their debit or credit card.

Remote purchase (CNP) fraud losses 2013-2022



Remote purchase (CNP) fraud case volumes 2013-2022

Year	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Cases	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	2,221,045
Change	27%	7%	9%	29%	-3%	47%	5%	12%	0%	-8%

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	+ 1%	VOLUME	19,594	- 21%
--------------	--------------	-------------	---------------	---------------	--------------

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

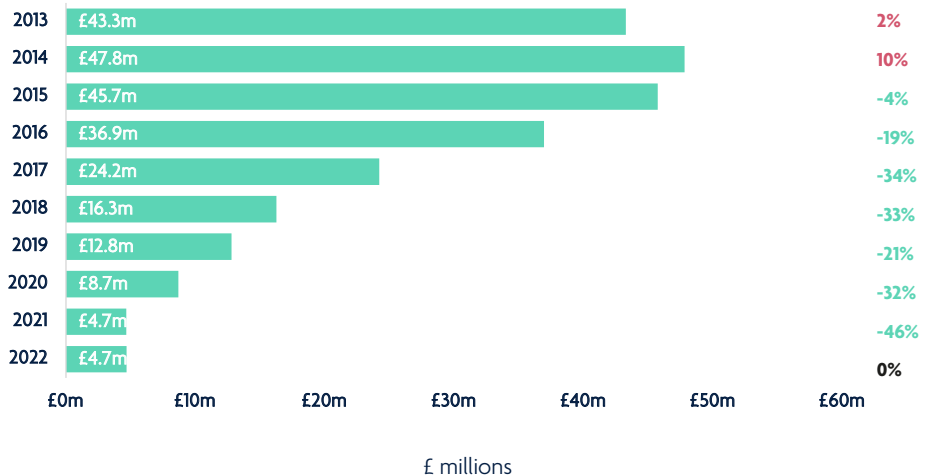
Counterfeit card losses totalled £4.7 million in 2022, a rise of less than one per cent on the total reported in 2021, 97 per cent lower than the peak for this category reported in 2008 (£169.8 million). Case volumes fell by 21 per cent to 19,594, the lowest total on record since data collection began.

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 continuous decrease in this type of fraud since 2008 is a result of the introduction of chip technology in the UK and its subsequent increased adoption around the world which has restricted fraudsters use of the counterfeit cards.

Counterfeit card fraud losses 2013-2022



Counterfeit card fraud case volumes 2013-2022

Year	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Cases	101,109	99,279	86,021	108,597	85,025	58,636	65,907	52,782	24,908	19,594
Change	3%	-2%	-13%	26%	-22%	-31%	12%	-20%	-53%	-21%

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 **£100.2m** **+ 30%**

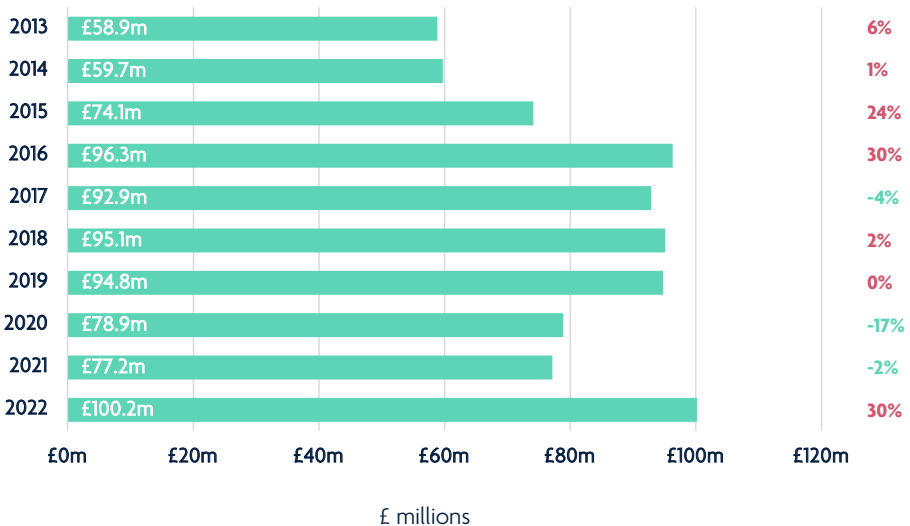
VOLUME **401,343** **+ 23%**

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. Typically, this involves obtaining cards through low-tech methods such as distraction thefts and entrapment devices attached to ATMs.

Losses due to lost and stolen card fraud increased 30 per cent in 2022 and totalled £100.2 million. For the first time on record, losses for this category have exceeded £100 million. There was also a rise in the number of incidents reported, increasing 23 per cent to 401,343 cases. Rises were expected in 2022 given the increases to contactless limits during the pandemic and also the increased acceptance of contactless, which accelerated during the Covid-19 lockdowns.

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 2013-2022



Lost and stolen card fraud case volumes 2013-2022

Year	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Cases	138,967	133,943	143,802	231,164	350,279	434,991	460,142	321,994	325,501	401,343
Change	23%	-4%	7%	61%	52%	24%	6%	-30%	1%	23%

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

£51.7m

+ 97%

VOLUME

82,064

+ 105%

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.

Both types of fraud associated with Card ID theft require the compromise of significant amounts of customers' personal information which is then used to impersonate victims.

It is believed that the increase behind this type of fraud is a result of fraudsters focused efforts to target victims' personal information using methods including phishing emails, scam texts and the theft of mail from external mailboxes and multi-occupancy buildings

Third-party application

Value - £17.3 million (+59%)

Volume 16,687 (+3%)

With third-party application fraud, a criminal will use stolen or fake documents to open a card account in someone else's name. This information will typically have been gathered through data loss, such as via data hacks and social engineering to compromise personal data.

which is then used to target the customers' existing accounts or apply for credit cards by impersonating the victim.

Losses from card ID theft increased 97 per cent in 2022 compared with 2021, totalling £51.7 million. The number of individual cases more than doubled over the same period to 82,064; both totals are the highest ever recorded for this category.

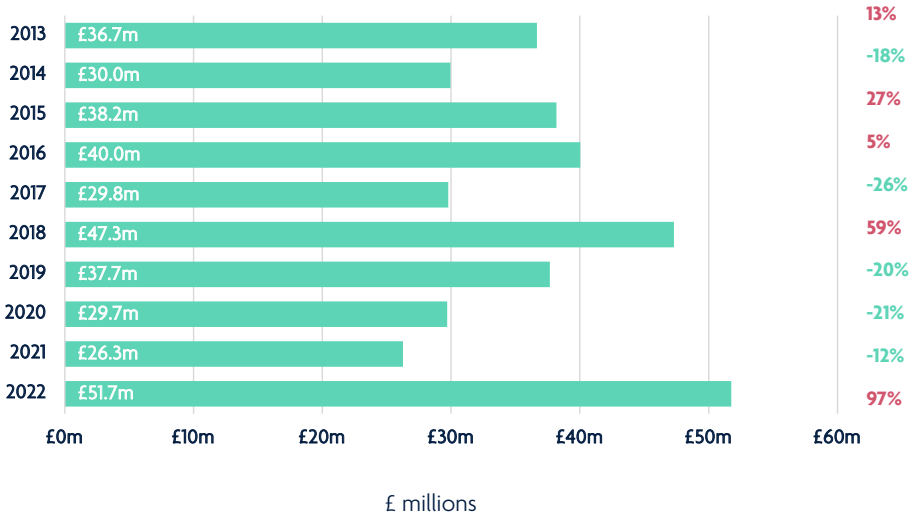
Account takeover

Value - £34.5 million (+124%)

Volume 65,377 (+174%)

In an account takeover fraud, a criminal takes over another person's genuine card account.

Card ID Theft Fraud Losses 2013-2022



Card ID theft fraud case volumes 2013-2022

Year	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Cases	30,718	26,542	33,566	31,756	29,156	63,791	54,165	34,545	40,026	82,064
Change	26%	-14%	26%	-5%	-8%	119%	-15%	-36%	16%	105%

How to stay safe from card ID fraud:

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

CARD NOT RECEIVED FRAUD

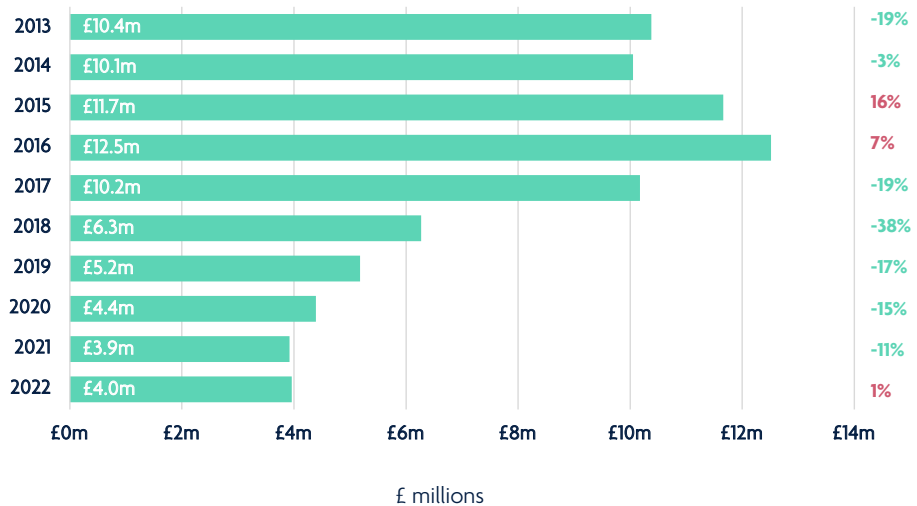
VALUE	£4.0m	+1%	VOLUME	8,848	-1%
--------------	--------------	------------	---------------	--------------	------------

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 increased by one per cent to £4 million in 2022. The volume of cases fell by one per cent, indicating the static nature of this type of fraud.

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 not

get their mail redirected when they change address are also vulnerable to this type of fraud.

Card not received fraud losses 2013-2022



Card not received fraud case volumes 2013-2022

Year	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Cases	9,125	9,302	10,719	11,377	10,903	10,046	7,907	8,435	8,941	8,848
Change	1%	2%	15%	6%	-4%	-8%	-21%	7%	6%	-1%

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	£72.0m	+54%
--------------	---------------	-------------

UK retail face-to-face card fraud covers all transactions that occur in person in a UK shop. Fraud losses on face-to-face purchases on the UK high street increased 54 per cent in 2022 to £72 million. Given the extended periods in 2021 when many shops were closed due to Covid-19 restrictions, a rise had been expected in 2022.

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 £34.9million in 2022, a rise of 82 per cent when compared to 2021. However, it should be noted that early 2021 saw reduced opportunities for fraudsters to commit

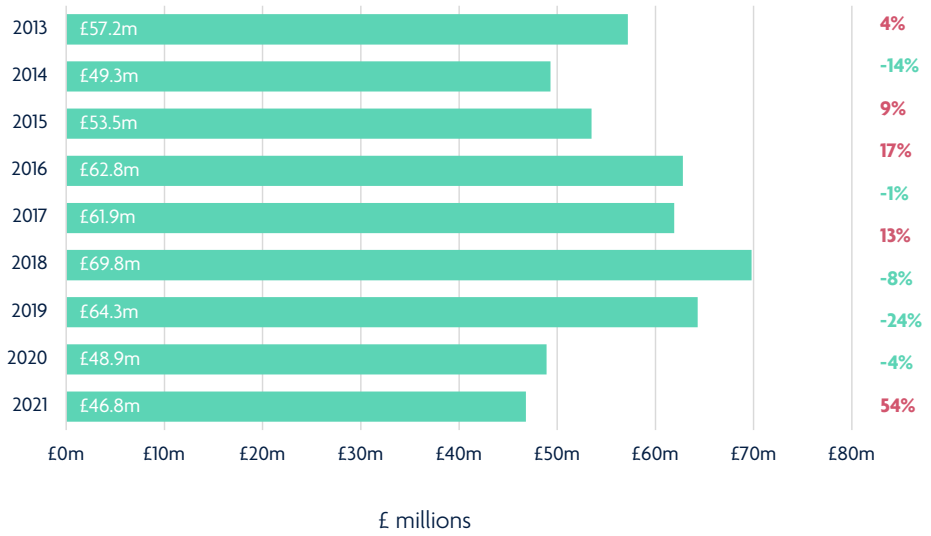
these types of scams because of Covid-19 lockdowns, meaning year on year comparisons should be viewed in the context of these restrictions.

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.

Contactless fraud on payment cards and devices represents only six 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 2013-2022



INTERNET/E-COMMERCE FRAUD

VALUE **£285.2m** **- 16%**

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.

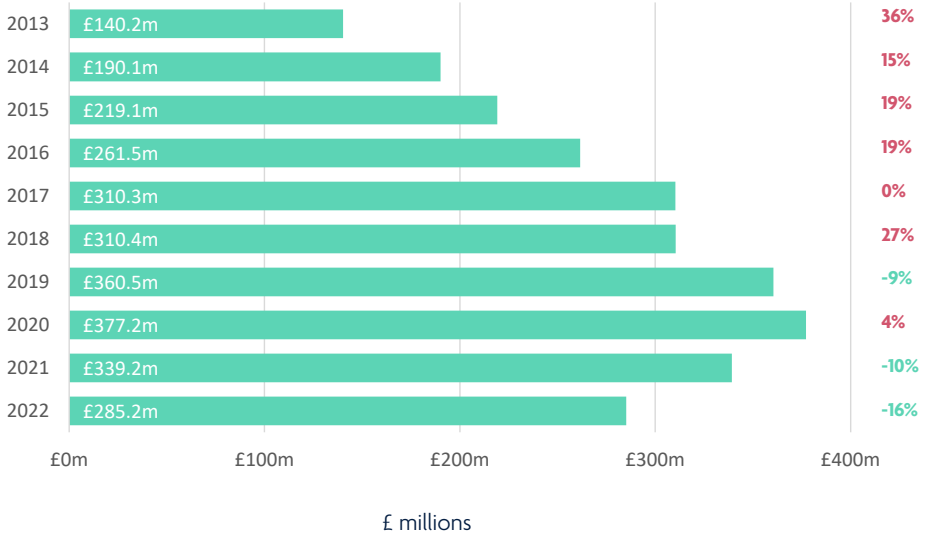
An estimated £285.2million of e-commerce fraud took place on cards in 2022, accounting for just over half of all card fraud and 72 per cent of total remote purchase fraud.

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 losses on UK issued cards 2013-2022



CARD FRAUD AT UK CASH MACHINES

VALUE **£26.1m** **+7%**

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.

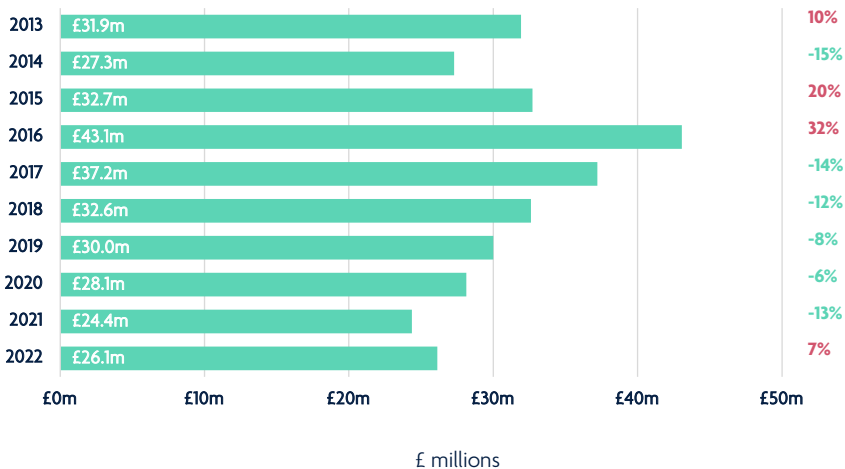
Fraudsters also target cash machines to compromise or steal cards or card details in three main ways:

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.

UK ATM losses on UK issued cards 2013-2022



CARD FRAUD ABROAD

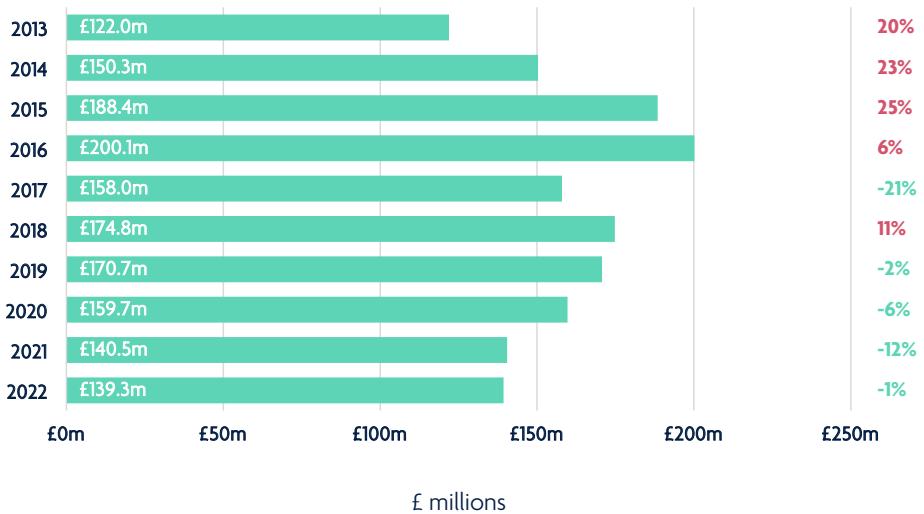
VALUE **£139.3m** **- 1%**

This category covers fraud occurring in locations overseas on UK-issued cards. International fraud losses for 2022 were £139.3 million, the lowest total reported since 2013 and 39 per cent lower than when compared with losses at their peak in 2008 (£230.1 million).

Almost three quarters (72 per cent) of this type of fraud is attributed to remote purchase fraud at overseas retailers.

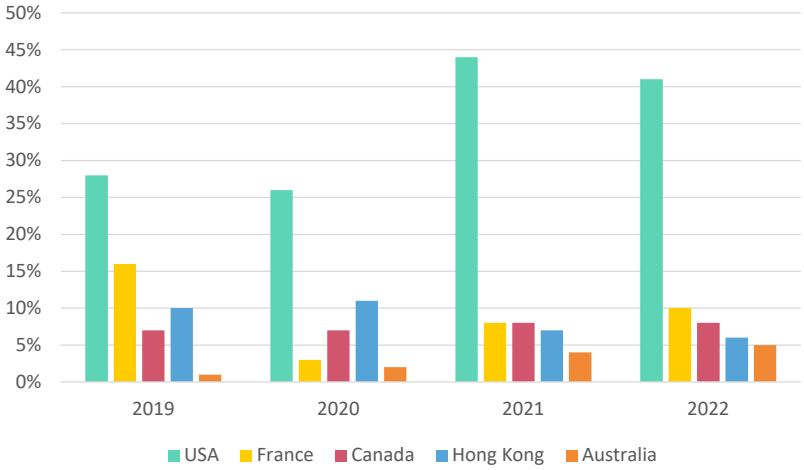
This category also includes cases where criminals steal the magnetic stripe details from UK-issued cards to make counterfeit cards which are used overseas in countries yet to upgrade to Chip and PIN.

International fraud losses on UK issued cards 2013-2022



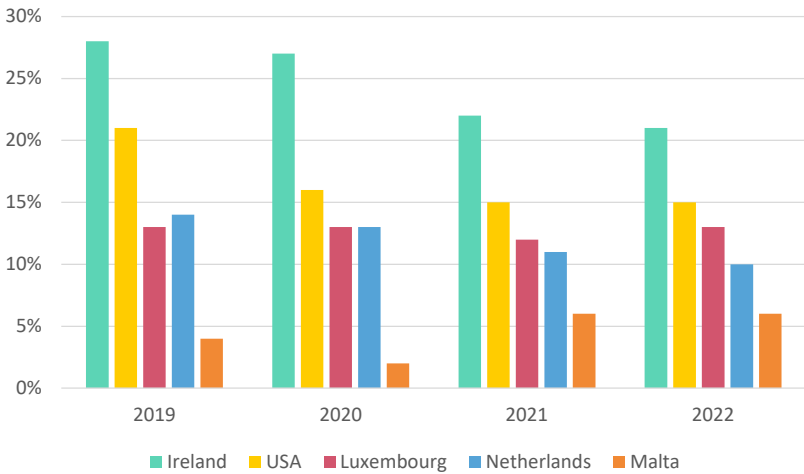
Top five countries for fraud on foreign-issued cards occurring in the UK 2018-2022

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 2018-2022

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





CHEQUE FRAUD

UNAUTHORISED CHEQUE FRAUD

VALUE	£7.5m	+ 18%	VOLUME	966	+ 19%
--------------	--------------	--------------	---------------	------------	--------------

Cheque fraud losses increased to £7.5 million in 2022, a rise of 18 per cent when compared to 2021. Meanwhile the volume of fraudulent cheques increased by 19 per cent.

It should be noted that the volume and value of cheque fraud remains very low, and while increases have been reported in 2022, they are not considered to be significant.

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.

Just under £20 million of cheque fraud was prevented in 2022 by the industry.

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

Counterfeit cheque fraud - £1.8million (-31%)

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

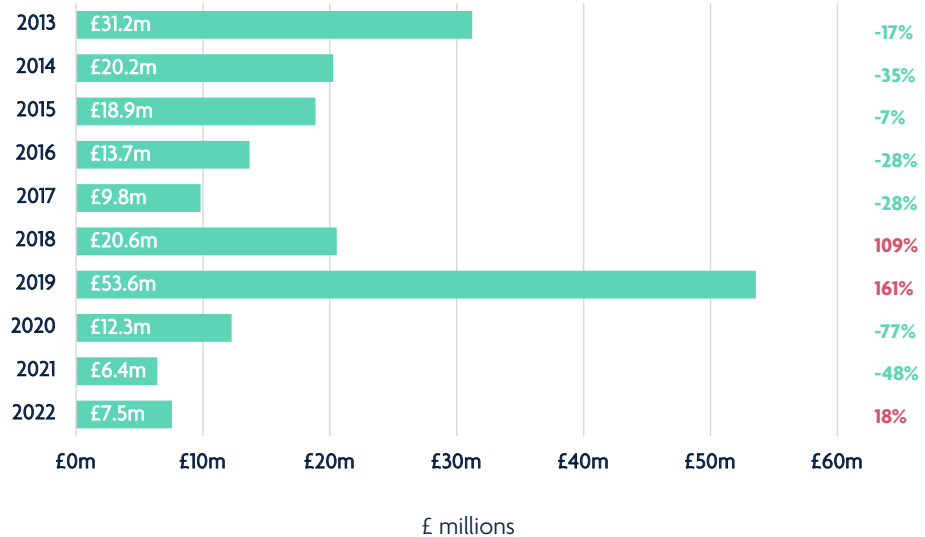
Fraudulently altered cheques - £3.3million (+110%)

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 – £2.4million (+11%)

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

Cheque fraud losses 2013-2022



Cheque fraud case volumes 2013-2022

Year	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Cases	10,471	8,168	5,746	3,388	1,745	2,020	2,852	1,247	815	966
Change	-33%	-22%	-30%	-41%	-48%	16%	41%	-56%	-35%	19%

How to stay safe from card not received 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

UNAUTHORISED REMOTE BANKING FRAUD

VALUE **£163.1m**

- 18%

VOLUME **47,473**

- 46%

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 £163.1 million in 2022, 18 per cent lower than in 2021. The number of cases of remote banking fraud also decreased, falling by 46 per cent to 47,473. It is worth noting that this type of fraud peaked in 2021 (£199.5 million) and a reduction was expected as lockdown restrictions eased, and life returned to some form of normality.

A total of £174 million of attempted remote banking fraud was stopped by bank security systems during 2022. This is equivalent to 51.6p in every £1 of fraud attempted being prevented.

In addition, 12 per cent (£19.9 million) of the losses across all remote banking channels were recovered after the incident.

In 2022, 86 per cent of the adult population used at least one form of remote banking.

Remote banking fraud losses 2013 – 2022

Channel	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	% Change 21/22
Internet Banking	£58.8m	£81.4m	£133.5m	£101.8m	£121.2m	£123.0m	£111.8m	£159.7m	£158.3m	£114.1m	-28%
Telephone Banking	£13.1m	£16.8m	£32.3m	£29.6m	£28.4m	£22.0m	£23.6m	£16.1m	£15.5m	£14.7m	-5%
Mobile Banking	N/A	N/A	£2.8m	£5.7m	£6.5m	£7.9m	£15.2m	£21.6m	£25.8m	£34.2m	33%
Total	£71.7m	£71.9m	£98.2m	£137.0m	£156.1m	£152.9m	£150.7m	£197.3m	£199.5m	£163.1m	-18%

Remote banking case volumes 2013 – 2022

Channel	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	% Change 21/22
Internet Banking	13,799	16,041	19,691	20,088	21,745	20,904	25,849	55,995	72,557	32,036	-56%
Telephone Banking	5,596	5,778	11,380	10,495	9,577	7,937	11,199	7,490	4,623	3,076	-33%
Mobile Banking	N/A	N/A	2,235	2,809	3,424	2,956	6,872	10,155	11,270	12,361	10%
Total	19,395	21,819	33,306	33,392	34,746	31,797	43,920	73,640	88,450	47,473	-46%

*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 **£114.1 m** **- 28%**

VOLUME **32,036** **- 56%**

This type of fraud occurs when a fraudster gains access to a customer's bank account through internet banking using compromised personal details and passwords 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 impersonation scam calls, emails or text messages typically exploiting current affairs (Covid-19, cost-of-living support etc) 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.

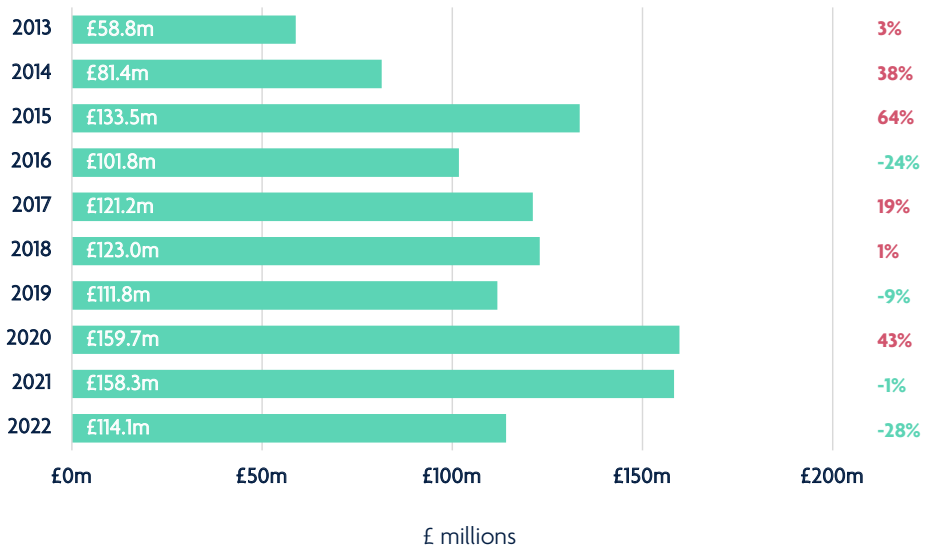
Criminals also abuse remote access software applications to gain control of their victim's online banking facilities. The criminals will typically claim to be providing support from an IT service or internet service provider and convince the customer to download and install remote access applications to their laptop or PC.

Internet banking fraud losses decreased in 2022, falling 28 per cent to £114.1 million when compared with 2021. Case volumes also fell by 56 per cent to 32,036. A main driver behind the reduction is the prevalence of this type during Covid-19 lockdowns, when many people would have been working from home, spending longer online, and doing more internet shopping. This provided criminals with greater opportunities to trick people into revealing their security information. These opportunities have therefore reduced as restrictions have ended.

A total of £117.4 million of attempted internet banking fraud was stopped by bank security systems during 2022. This is equivalent to 51p in every £1 of fraud attempted being prevented.

In addition, 14 per cent (£16.2 million) of the losses across the internet banking channel were recovered after the incident.

Internet banking fraud losses 2013 – 2022



Internet banking case volumes 2013 – 2022

Year	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	
Cases	13,799	16,041	19,691	20,088	21,745	20,904	25,849	55,995	72,557	32,036	
Change		-16%	16%	23%	2%	8%	-4%	24%	117%	30%	-56%

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	£14.7m	- 5%	VOLUME	3,076	- 33%
--------------	---------------	-------------	---------------	--------------	--------------

This type of fraud occurs when a criminal uses compromised bank account details to gain access to a customer’s telephone banking account and makes an unauthorised transfer of money away from it.

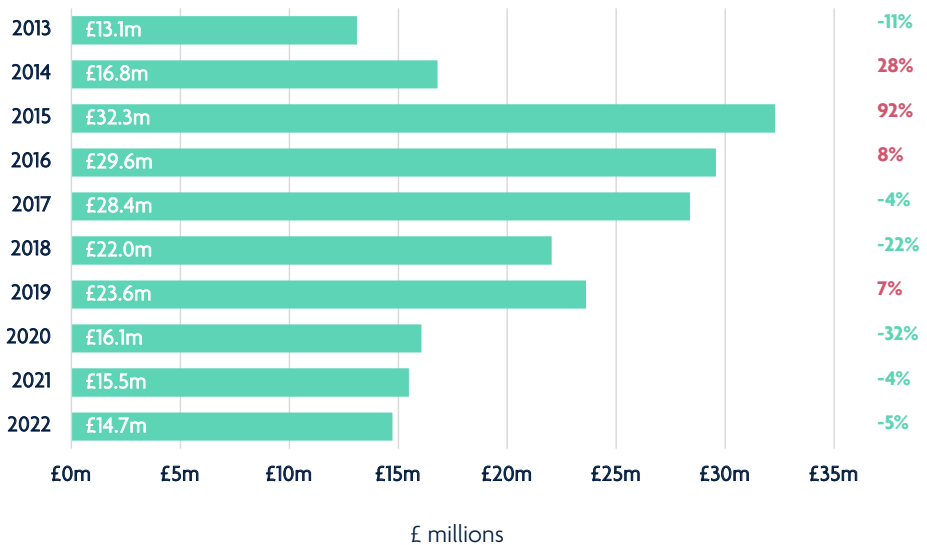
Like internet banking fraud, criminals often use social engineering tactics to trick customers into revealing their account security details, which are then used to convince the telephone banking operator that they are the genuine account holder.

Losses from telephone banking fraud decreased by five per cent to £14.7 million in 2022, the lowest recorded total since 2013. The number of cases decreased by 33 per cent to 3,076.

A total of £27.1 million of attempted telephone banking fraud was stopped by bank security systems during 2022. This is equivalent to 65p in every £1 of fraud attempted being prevented.

In addition, eight per cent (£1.3 million) of the losses across the telephone banking channel were recovered after the incident.

Telephone banking fraud losses 2013 – 2022



Telephone banking case volumes 2013 – 2022

Year	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Cases	5,596	5,778	11,380	10,495	9,577	7,937	11,199	7,490	4,623	3,076
Change	-21%	3%	97%	-8%	-9%	-17%	41%	-33%	-38%	-33%

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 **£34.2m** **+ 33%**

VOLUME **12,361** **+ 10%**

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.

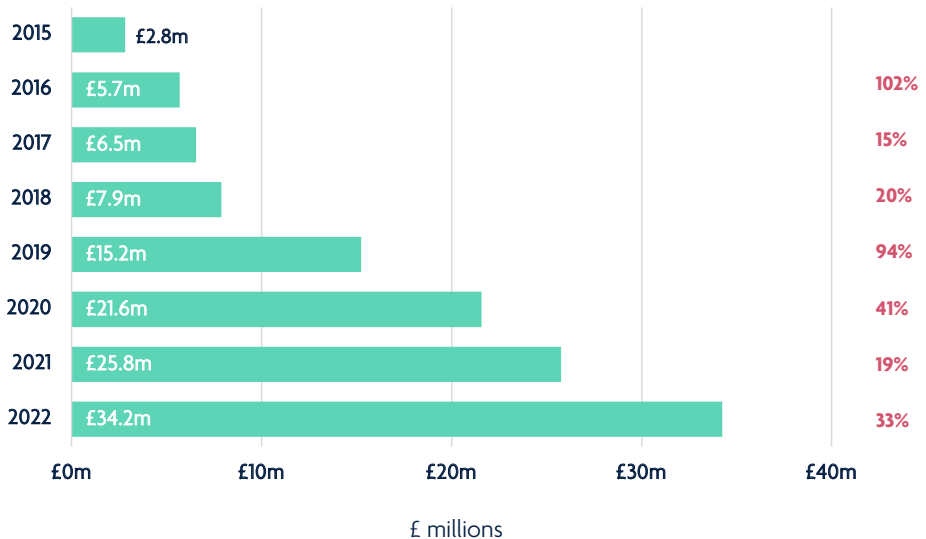
It excludes web browser banking on a mobile and browser-based banking apps (incidents on those platforms are included in the internet banking fraud figures).

Rises are to be expected in the mobile banking channel as the level of usage increases amongst customers. Around 53 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 £29.6 million of attempted mobile banking fraud was stopped by bank security systems during 2022. This is equivalent to 46p in every £1 of fraud attempted being prevented.

In addition, seven per cent (£2.3 million) of the losses across the mobile banking channel were recovered after the incident.

Mobile banking fraud losses 2013 – 2022



Mobile banking case volumes 2013 – 2022

Year	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Cases	N/A	N/A	2,235	2,809	3,424	2,956	6,872	10,155	11,270	12,361
Change				26%	22%	-14%	132%	48%	11%	10%

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 is a scam. Instead, contact the company directly using a known email or phone number.



AUTHORISED FRAUD

AUTHORISED PUSH PAYMENT (APP) FRAUD

VALUE	£485.2m	- 17%	VOLUME	207,372	+ 6%
-------	---------	-------	--------	---------	------

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 £485.2 million in 2022. This was split between personal (£408.2 million) and non-personal or business (£77 million).

In total there were 207,372 cases. Of this total, 200,643 cases were on personal accounts and 6,729 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 remains a key driver behind the losses. 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. The Payment Systems Regulator (PSR) is currently consulting on proposals that would require payment service providers to reimburse losses in all but exceptional cases.

All APP cases reported 2020-2022

		PERSONAL				NON PERSONAL				TOTAL			
		2020	2021	2022	Change	2020	2021	2022	Change	2020	2021	2022	Change
Volume	Cases	145,207	188,964	200,643	6%	9,407	7,032	6,729	-4%	154,614	195,996	207,372	6%
	Payments	228,946	333,751	361,761	8%	15,625	11,386	10,505	-8%	244,571	345,137	372,266	8%
Value	Value	£347.4m	£505.9m	£408.2m	-19%	£73.3m	£77.4m	£77.0m	0%	£420.7m	£583.2m	£485.2m	-17%
	Repatriation	£163.4m	£246.8m	£254.1m	3%	£27.4m	£24.4m	£31.5m	30%	£190.8m	£271.2m	£285.6m	5%

- **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.

FRAUD ORIGINATION

Our annual reporting of fraud statistics draws information from banks and payment service providers on identified and reported fraudulent activity. It concentrates on the prevalence and nature of different fraud and scams types, as well as the losses incurred. This enables the industry and stakeholders to monitor change over time, informing ongoing detection and prevention strategies.

But the vast majority of fraudulent activity starts outside the banking sector. Key to tackling and ultimately reducing losses and the impact on consumers, is greater understanding on where and how fraud and scams originate.

For the first time UK Finance is publishing data which sheds new light on the source of authorised push payment fraud. We can do this through analysis of a subset of APP data which uses anonymised case data that includes insight on the reported origination of fraud events.

This shows that:

- 78% of fraud cases originate from online sources. These cases tend to include lower-value scams such as purchase fraud and therefore account for 36% of total losses,
- 18% of fraud cases originate from telecommunications, these are usually higher value cases such as impersonation scams and so account for 44% of losses

The analysis is based on information provided by victims of fraud and then reported by UK Finance members. A further explanation of how the data is gathered and the methodology is included below.

6 months: 1st July 2022 to 31st December 2022		
	Volume	Value
Online	78%	36%
Telecommunications	18%	44%
Email	2%	12%
Other	2%	7%

The Data:

- The Best Practice Standards (BPS) system is a secure platform which allows its members – which include, national and regional, domestic and international, physical and virtual, banks and non-banks, as well as payment service providers – to share information relating to fraud and ‘push payment’ scams.
- The BPS platform enables firms to create cases in real-time, quickly passing information to other financial institutions that have received fraudulent money. This greatly increases the chances of being able to freeze it and stop it ending up in a criminal’s hands.
- UK Finance has access to aggregate reporting from the BPS system, allowing it to assess the volume and value of fraud and scams and the origination of the fraudulent activity, as reported by the victim. Aggregate information is compiled only once members have investigated the fraudulent activity and cases are closed. UK Finance does not have access to individual case information and is therefore unable to make an assessment as to the accuracy of the data included and no quality assurance checks are undertaken on the data inputs. However, extensive testing, engagement with members during the development of the system, and validation with other sources of fraud data allows the conclusion that the extracted data are consistent with industry trends.
- The data presented provide a statement of the origination of fraud and scams during the stated periods, noting that the victim will not, in every case, be aware of where the initial compromise happened, and as such these figures cannot be considered definitive. Only information relating to cases that have been closed are loaded to the BPS platform, so not all incidents of scams will be included here. For more detail on these please refer to the UK Finance Annual Fraud Report.
- Data may be subject to future restatement if further information becomes available.

APP VOLUNTARY CODE*

*The figures quoted below are included within the overall APP total in the previous section and should therefore not be treated as an addition to the overall numbers.

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 2022, 190,675 cases were assessed and closed with a total value of £376.1 million. Our latest figures show that £248.6 million of losses were returned to victims under the APP voluntary code, accounting for 66 per cent of losses in these cases.

		< £1k	> £1k < £10k	> £10k	Total
Volume	Cases	142,013	42,314	6,348	190,675
	Payments	196,428	101,040	42,976	340,444
Value	Value	£35.8m	£126.7m	£213.6m	£376.1m
	Repatriation	£23.8m	£78.1m	£131.9m	£248.6m**

** This includes £14.7million 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.

FURTHER ANALYSIS OF THE APP SCAM DATA

UK Finance collates enhanced data which provide further insight into APP scams. This data covers:

- **Eight scam types:** malicious payee (purchase scam, investment scam, romance scam and advance fee scam) and malicious redirection (invoice and mandate scam, CEO fraud, impersonation: police/bank staff and impersonation: other).
- **Six payment types:** faster payment, CHAPS, BACS (payment), BACS (standing order), intrabank (“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 **£67m**

+ 4%

VOLUME **117,170**

+ 17%

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 2022, with 117,170 cases accounting for 57 per cent of the total number of APP scam cases. A total of £67 million was lost to purchase scams in 2022, with the vast majority of losses being from personal accounts. Payment service providers were subsequently able to return £38.1 million of the losses.

All purchase scam cases reported 2020 – 2022

		PERSONAL				NON PERSONAL				TOTAL			
		2020	2021	2022	Change	2020	2021	2022	Change	2020	2021	2022	Change
Volume	Cases	80,214	97,382	114,417	17%	4,078	2,351	2,753	17%	84,292	99,733	117,170	17%
	Payments	102,325	129,442	155,451	20%	5,168	2,969	3,667	24%	107,493	132,411	159,118	20%
Value	Value	£44.7m	£56.8m	£59.6m	5%	£6.5m	£7.4m	£7.4m	0%	£51.1m	£64.1m	£67.0m	4%
	Repatriation	£14.2m	£20.0m	£35.3m	77%	£1.7m	£2.1m	£2.8m	33%	£15.9m	£22.1m	£38.1m	73%

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	98,202	10,196	566	108,964
	Payments	126,975	19,158	2,075	148,208
Value	Value	£19.7m	£27.9m	£11.3m	£58.9m
	Repatriation	£13.1m	£13.7m	£6.5m	£33.2m

For those cases which were applicable for assessment using the voluntary code in 2022, 56 per cent of all losses were returned to the victim compared with 34 per cent in 2021. 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.

INVESTMENT SCAM

VALUE **£114.1m** **- 34%**

VOLUME **10,085** **- 16%**

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 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. Adverts on social media usually offering unrealistic returns, and letters are also used heavily in investment scams.

Investment scam losses decreased by more than a third in 2022: this is likely a combination of factors including fewer opportunities for fraudsters to contact victims now that lockdown restrictions have eased, and also the emergence of cost of living pressures meaning individuals are more cautious with money and less likely to be looking for investment opportunities. Investment scams

still accounted for the largest value of all eight APP scam types in 2022, a continuation of the trend seen in 2020 and 2021 with losses of £114.1 million or 24 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 scams account for the largest proportion of loss, they only account for five per cent of the total number of APP scam cases. Payment services providers were subsequently able to return £58.6 million to victims or 51 per cent of the total.

All investment scam cases reported 2020 – 2022

		PERSONAL				NON PERSONAL				TOTAL			
		2020	2021	2022	Change	2020	2021	2022	Change	2020	2021	2022	Change
Volume	Cases	7,900	11,905	9,941	-16%	281	169	144	-15%	8,181	12,074	10,085	-16%
	Payments	19,322	35,071	30,065	-14%	601	594	446	-25%	19,923	35,665	30,511	-14%
Value	Value	£103.6m	£166.2m	£109.3m	-34%	£5.8m	£5.5m	£4.8m	-13%	£109.4m	£171.7m	£114.1m	-34%
	Repatriation	£39.0m	£72.7m	£56.9m	-22%	£1.2m	£2.0m	£1.7m	-15%	£40.2m	£74.6m	£58.6m	-21%

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	4,358	2,563	1,502	8,423
	Payments	7,258	7,849	9,199	24,306
Value	Value	£1.5m	£8.9m	£69.6m	£79.9m
	Repatriation	£0.9m	£4.5m	£40.1m	£45.5m

For only those cases which were applicable for assessment using the voluntary code, 57 per cent of all losses were returned to the victim in 2022 compared with 45 per cent 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](https://www.fca.org.uk) or register.fca.org.uk. Ensure you only use the contact details listed on the Register to confirm you're dealing with the genuine firm before parting with your money and information.
- You can check if an investment or pension opportunity you've been offered could potentially be a scam by taking the FCA's ScamSmart test.
- Report scam ads appearing in paid-for space online by visiting the Advertising Standard Authority's website where you can complete their quick reporting form.

ROMANCE SCAM

VALUE **£31.3m**

+ 1%

VOLUME **3,649**

+ 12%

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 £31.3 million was lost to romance scams in 2022, an increase of one per cent when compared to 2021.

Romance scams have an average of over eight scam payments per case; 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.

Payment services providers were subsequently able to return £16.4 million to victims or 52 per cent of the total.

All romance scam cases reported 2020 – 2022

	PERSONAL				NON PERSONAL				TOTAL				
	2020	2021	2022	Change	2020	2021	2022	Change	2020	2021	2022	Change	
Volume	Cases	2,252	3,245	3,617	11%	73	25	32	28%	2,325	3,270	3,649	12%
	Payments	12,778	25,723	30,119	17%	407	91	101	11%	13,185	25,814	30,220	17%
Value	Value	£17.3m	£30.6m	£30.9m	1%	£0.5m	£0.3m	£0.4m	28%	£17.8m	£30.9m	£31.3m	1%
	Repatriation	£6.5m	£12.4m	£16.3m	31%	£0.1m	£0.2m	£0.2m	-17%	£6.6m	£12.6m	£16.4m	31%

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	1,406	1,299	553	3,258
	Payments	3,982	9,959	13,258	27,199
Value	Value	£0.5m	£4.6m	£21.4m	£26.4m
	Repatriation	£0.3m	£2.7m	£11.3m	£14.3m

For only those cases which were applicable for assessment using the voluntary code, 54 per cent of all losses were returned to the victim in 2022 compared with 44 per cent 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.

ADVANCE FEE SCAM

VALUE **£32.2m** **+ 0%**

VOLUME **27,329** **+ 33%**

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 as a deposit for high-value goods and holidays.

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 on social media or with an email, or a letter sent by the criminal to the victim.

Advance fee scams were the third most common form of APP scam in 2022, accounting for 13 per cent of the total number of cases. A total of £32.2 million was lost to advance fee scams last year, an increase of less than one percent compared to 2021.

All advance fee scam cases reported 2020 – 2022

		PERSONAL				NON PERSONAL				TOTAL			
		2020	2021	2022	Change	2020	2021	2022	Change	2020	2021	2022	Change
Volume	Cases	13,316	19,950	26,871	35%	517	545	458	-16%	13,833	20,495	27,329	33%
	Payments	22,434	36,166	50,463	40%	798	804	768	-4%	23,232	36,970	51,231	39%
Value	Value	£21.2m	£30.8m	£30.7m	0%	£1.0m	£1.4m	£1.5m	11%	£22.2m	£32.1m	£32.2m	0%
	Repatriation	£7.4m	£10.9m	£17.2m	63%	£0.3m	£0.9m	£0.6m	-33%	£7.7m	£11.8m	£17.8m	50%

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	20,847	4,295
	Payments	34,027	10,682	3,355	48,064
Value	Value	£5.2m	£10.6m	£12.8m	£28.6m
	Repatriation	£3.4m	£4.7m	£7.0m	£15.1m

For only those cases which were applicable for assessment using the voluntary code, 53 per cent of all losses were returned to the victim in 2022 compared with 34 per cent 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, for example 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's 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.

INVOICE AND MANDATE SCAM

VALUE **£49.5m** **- 13%**

VOLUME **3,340** **- 23%**

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 scam losses totalled £49.5 million in 2022, a decrease of 13 per cent when compared to 2021. 70 per cent (£34.5 million) of invoice and mandate scam losses occurred on a non-personal or business account. Typically, businesses make genuine higher-value payments more regularly, making it harder to spot and stop a fraudulent one. Payment services providers were subsequently able to return £26.4 million to victims or 53 per cent of the total.

All invoice and mandate scam cases reported 2020 – 2022

		PERSONAL				NON PERSONAL				TOTAL			
		2020	2021	2022	Change	2020	2021	2022	Change	2020	2021	2022	Change
Volume	Cases	2,903	2,555	1,871	-27%	1,818	1,775	1,469	-17%	4,721	4,330	3,340	-23%
	Payments	3,904	3,676	2,836	-23%	2,416	2,491	2,129	-15%	6,320	6,167	4,965	-19%
Value	Value	£25.1m	£19.9m	£15.0m	-25%	£43.6m	£36.8m	£34.5m	-6%	£68.8m	£56.7m	£49.5m	-13%
	Repatriation	£15.7m	£12.6m	£12.4m	-2%	£16.1m	£10.2m	£14.0m	30%	£31.8m	£22.8m	£26.4m	16%

Only those cases assessed using the voluntary code by signatory PSPs

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

		< £1k	> £1k < £10k	> £10k	Total
Volume	Cases	675	1,334	422	2,431
	Payments	827	1,817	873	3,517
Value	Value	£0.3m	£4.5m	£17.6m	£22.5m
	Repatriation	£0.2m	£3.1m	£10.9m	£14.3m

For only those cases which were applicable for assessment using the voluntary code, 62 per cent of all losses were returned to the victim in 2022 compared with 61 per cent in 2021.

How to stay safe from invoice and mandate scams:

- Always confirm any bank account details directly with the company either on the telephone or in person before you make a payment or transfer any money.
- Criminals can access or alter emails to make them look genuine. Do not use the contact details in an email, instead check the company's official website or documentation.
- If you are making a payment to an account for the first time, transfer a small sum first and then check with the company using known contact details that the payment has been received to check the account details are correct.
- Contact your bank straight away if you think you may have fallen for an invoice or mandate scam.

CEO SCAM

VALUE **£13.4m** **+ 6%**

VOLUME **432** **- 6%**

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 2022, accounting for less than one per cent of total cases. A total of £13.4 million was lost, equivalent to only three per cent of total APP losses.

All CEO scam cases reported 2020 – 2022

		PERSONAL				NON PERSONAL				TOTAL			
		2020	2021	2022	Change	2020	2021	2022	Change	2020	2021	2022	Change
Volume	Cases	82	65	50	-23%	275	396	382	-4%	357	461	432	-6%
	Payments	127	99	80	-19%	360	579	535	-8%	487	678	615	-9%
Value	Value	£0.9m	£1.1m	£0.6m	-49%	£3.9m	£11.6m	£12.9m	11%	£4.8m	£12.7m	£13.4m	6%
	Repatriation	£0.5m	£0.7m	£0.3m	-50%	£1.5m	£2.4m	£3.2m	33%	£2.0m	£3.1m	£3.6m	17%

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	14	112
	Payments	16	145	126	287
Value	Value	£0.0m	£0.5m	£3.2m	£3.7m
	Repatriation	£0.0m	£0.2m	£1.2m	£1.5m

For only those cases which were applicable for assessment using the voluntary code, 41 per cent of all losses were returned to the victim in 2022 compared with 57 per cent in 2021.

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.

IMPERSONATION: POLICE/BANK STAFF SCAM

VALUE	£109.8m	- 20%	VOLUME	16,948	- 42%
--------------	----------------	--------------	---------------	---------------	--------------

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.

Police and bank staff impersonation scams accounted for 23 per cent of all APP scam losses in 2022 totalling £109.8 million; the second highest of the eight APP scam types. However, losses have decreased by 20 per cent when compared to 2021 and case volumes have fallen by 42 per cent in the same period. This is likely to be a result of the decreased opportunities for criminals to contact victims since lockdown restrictions were lifted.

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.

Payment service providers were able to return £82.3 million of the losses to customers or 75 per cent of the total.

All impersonation: police/bank staff scam cases reported 2020 – 2022

		PERSONAL				NON PERSONAL				TOTAL			
		2020	2021	2022	Change	2020	2021	2022	Change	2020	2021	2022	Change
Volume	Cases	20,199	28,629	16,413	-43%	978	777	535	-31%	21,177	29,406	16,948	-42%
	Payments	37,232	60,931	47,139	-23%	3,365	1,875	1,391	-26%	40,597	62,806	48,530	-23%
Value	Value	£84.3m	£130.3m	£100.7m	-23%	£6.6m	£7.0m	£9.1m	30%	£90.9m	£137.3m	£109.8m	-20%
	Repatriation	£53.9m	£80.7m	£76.0m	-6%	£4.2m	£4.1m	£6.3m	54%	£58.0m	£84.8m	£82.3m	-3%

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	4,358	9,442	2,210	16,010
	Payments	7,414	28,615	10,503	46,532
Value	Value	£2.3m	£37.3m	£60.8m	£100.4m
	Repatriation	£1.8m	£29.0m	£43.9m	£74.7m

For only those cases which were applicable for assessment using the voluntary code, 74 per cent of all losses were returned to the victim in 2022 compared with 60 per cent in 2021.

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](https://www.gov.uk).

IMPERSONATION SCAM: OTHER

VALUE **£67.8m** **- 13%**

VOLUME **28,419** **+ 8%**

In this scam, criminals claim 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 £67.8 million was lost to this type of scam in 2022, a reduction of 13 per cent when compared to 2021. Payment services providers were subsequently able to return £42.3 million to victims or 62 per cent of the total.

All impersonation: other scam cases reported 2020 – 2022

		PERSONAL				NON PERSONAL				TOTAL			
		2020	2021	2022	Change	2020	2021	2022	Change	2020	2021	2022	Change
Volume	Cases	18,341	25,233	27,463	9%	1,387	994	956	-4%	19,728	26,227	28,419	8%
	Payments	30,824	42,643	45,608	7%	2,510	1,983	1,468	-26%	33,334	44,626	47,076	5%
Value	Value	£50.4m	£70.1m	£61.3m	-13%	£5.4m	£7.4m	£6.5m	-13%	£55.8m	£77.5m	£67.8m	-13%
	Repatriation	£26.2m	£36.8m	£39.6m	8%	£2.3m	£2.6m	£2.7m	4%	£28.6m	£39.4m	£42.3m	7%

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	12,153	13,073	611	25,837
	Payments	15,929	22,815	3,587	42,331
Value	Value	£6.2m	£32.5m	£16.9m	£55.7m
	Repatriation	£4.2m	£20.2m	£11.0m	£35.3m

For only those cases which were applicable for assessment using the voluntary code, 63 per cent of all losses were returned to the victim in 2022 compared with 45 per cent in 2021.

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.

Payment Type	Number of Payments				Value			
	2020	2021	2022	CHANGE	2020	2021	2022	CHANGE
Faster Payment	236,641	335,451	364,964	9%	£349.4m	£504.5m	£421.1m	-17%
CHAPS	501	764	550	-28%	£14.5m	£22.5m	£13.9m	-38%
BACs	1,193	1,695	2,227	31%	£23.5m	£20.4m	£24.0m	17%
Intra Bank Transfer ("on us")	3,113	3,358	1,242	-63%	£10.6m	£7.5m	£1.5m	-80%
International	3,123	3,869	3,283	-15%	£22.7m	£28.3m	£24.7m	-13%
Total	244,571	345,137	372,266	8%	£420.7m	£583.2m	£485.2m	-17%

Faster Payments was used for 98 per cent of fraudulent APP scam payments. While CHAPS was the least common payment method, representing less than one per cent of cases, the high-value nature of transactions using this payment type meant that it accounted for three per cent of the total value.

PAYMENT CHANNEL

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

Payment Type	Number of Payments				Value			
	2020	2021	2022	CHANGE	2020	2021	2022	CHANGE
Branch	8,968	8,251	8,565	4%	£43.6m	£56.6m	£45.7m	-19%
Internet Banking	113,853	130,015	138,700	7%	£262.5m	£329.1m	£274.6m	-17%
Telephone Banking	5,593	6,249	6,176	-1%	£17.8m	£24.4m	£15.6m	-36%
Mobile Banking	116,157	200,622	218,809	9%	£96.9m	£173.2m	£149.3m	-14%
Total	244,571	345,137	372,250	8%	£420.7m	£583.2m	£485.2m	-17%

The most common payment channel was mobile banking which accounted for 59 per cent of the payment volume but only 31 per cent of the loss, indicating the typically lower payment limits available to customers within the mobile banking channel.

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>



CONTRIBUTING MEMBERS

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.

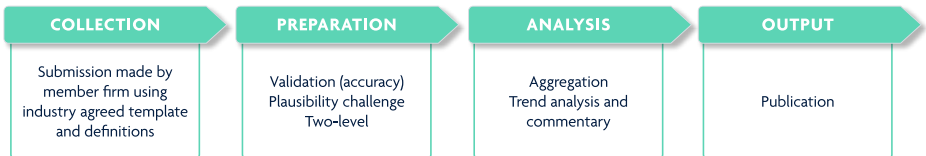
Data plausibility – outputs

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.

APPENDIX

CASES

TYPE	CATEGORY	SUB-CATEGORY	2020	2021	2022	CHANGE
UNAUTHORISED	CARD	Lost and stolen	321,994	325,501	401,343	23%
UNAUTHORISED	CARD	CNR	8,435	8,941	8,848	-1%
UNAUTHORISED	CARD	Counterfeit	52,782	24,908	19,594	-21%
UNAUTHORISED	CARD	Remote purchase	2,417,866	2,423,826	2,221,045	-8%
UNAUTHORISED	CARD	Card ID Theft	34,545	40,026	82,064	105%
UNAUTHORISED	CHEQUE	Cheque	1,247	815	966	19%
UNAUTHORISED	REMOTE BANKING	Internet Banking	55,995	72,557	32,036	-56%
UNAUTHORISED	REMOTE BANKING	Telephone Banking	7,490	4,623	3,076	-33%
UNAUTHORISED	REMOTE BANKING	Mobile Banking	10,155	11,270	12,361	10%
AUTHORISED	PAYMENT	Invoice and Mandate scam	4,721	4,330	3,340	-23%
AUTHORISED	PAYMENT	CEO scam	357	461	432	-6%
AUTHORISED	PAYMENT	Impersonation: Police/Bank	21,177	29,406	16,948	-42%
AUTHORISED	PAYMENT	Impersonation: Other	19,728	26,227	28,419	8%
AUTHORISED	PAYMENT	Purchase scam	84,292	99,733	117,170	17%
AUTHORISED	PAYMENT	Investment scam	8,181	12,074	10,085	-16%
AUTHORISED	PAYMENT	Romance scam	2,325	3,270	3,649	12%
AUTHORISED	PAYMENT	Advance Fee	13,833	20,495	27,329	33%
TOTAL	TOTAL	TOTAL	3,065,123	3,108,463	2,988,705	-4%

GROSS LOSSES

TYPE	CATEGORY	SUB-CATEGORY	2020	2021	2022	CHANGE
UNAUTHORISED	CARD	Lost & stolen	£78.9m	£77.2m	£100.2m	30%
UNAUTHORISED	CARD	CNR	£4.4m	£3.9m	£4.0m	1%
UNAUTHORISED	CARD	Counterfeit	£8.7m	£4.7m	£4.7m	1%
UNAUTHORISED	CARD	Remote purchase	£452.6m	£412.5m	£395.7m	-4%
UNAUTHORISED	CARD	Card ID Theft	£29.7m	£26.3m	£51.7m	97%
UNAUTHORISED	CHEQUE	Cheque	£12.3m	£6.4m	£7.5m	18%
UNAUTHORISED	REMOTE BANKING	Internet Banking	£159.7m	£158.3m	£114.1m	-28%
UNAUTHORISED	REMOTE BANKING	Telephone Banking	£16.1m	£15.5m	£14.7m	-5%
UNAUTHORISED	REMOTE BANKING	Mobile Banking	£21.6m	£25.8m	£34.2m	33%
AUTHORISED	PAYMENT	Invoice & Mandate scam	£68.8m	£56.7m	£49.5m	-13%
AUTHORISED	PAYMENT	CEO scam	£4.8m	£12.7m	£13.4m	6%
AUTHORISED	PAYMENT	Impersonation: Police/Bank	£90.9m	£137.3m	£109.8m	-20%
AUTHORISED	PAYMENT	Impersonation: Other	£55.8m	£77.5m	£67.8m	-13%
AUTHORISED	PAYMENT	Purchase scam	£51.1m	£64.1m	£67.0m	4%
AUTHORISED	PAYMENT	Investment scam	£109.4m	£171.7m	£114.1m	-34%
AUTHORISED	PAYMENT	Romance scam	£17.8m	£30.9m	£31.3m	1%
AUTHORISED	PAYMENT	Advance Fee	£22.2m	£32.1m	£32.2m	0%
TOTAL	TOTAL	TOTAL	£1204.6m	£1313.6m	£1212.1m	-8%

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.

© 2023, UK Finance