PSR Payment Systems Regulator

Unmasking how fraudsters target UK consumers in the digital age

December 2024

Contents

Executive summary

Preventing authorised push payment (APP) scams is one of our top priorities. APP scams cause immense suffering and harm to consumers and society, damage confidence in payments and lead to permanent loss of trust in institutions.

Our research[1] shows that victims' confidence in making payments drops after being a victim of an APP scam. A third say they have also lost confidence in using new payment methods. The need for action is clear, and we have taken decisive action to prevent APP scams across the payments industry.

We have done this by creating incentives for payment firms to improve scam prevention, through the publication of APP scams performance data[2] and through the introduction of a reimbursement requirement in October 2024, which requires victims of APP scams to be reimbursed by their bank when they fall victim to a scam.

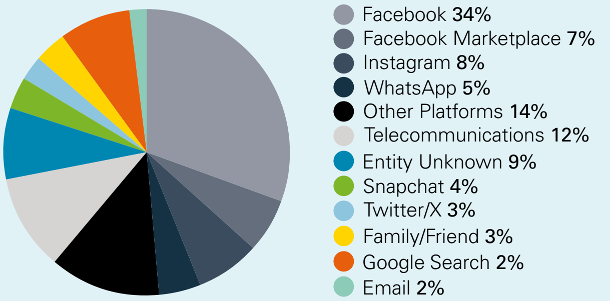
We want to do more to stop scams occurring in the first place, and this means working with other sectors as well as the payments industry. To make significant inroads to prevent APP scams, all ecosystem actors need to take action to prevent fraudsters contacting victims and earning their trust.

For this reason, we used our powers[3] this year to require the 14 largest banking groups in Great Britain and Northern Ireland to give us data on which platforms are most commonly reported as being exploited by fraudsters to make contact with victims, which later result in an APP scam, across different scam types. The scam types can be found on pages 6–7.

Key findings in our report

- Our data shows that fraudsters use major social media platforms, technology platforms, and the telecommunication sector to commit APP scams against UK consumers, leading to losses in the hundreds of millions.
- **According to our data[4], £341 million was lost to APP scams in 2023. Over half of these were reported by victims as originating on Meta platforms.** Meta platforms were recorded as being targeted by fraudsters to carry out 54% of the volume and 18% of the total value of APP scams. This means Meta platforms were used by fraudsters to carry out the loss of approximately £1 in every £5 lost in an APP scam.

Most common entities used by fraudsters (by volume)



- **Telecommunication and email[5] providers were recorded as being targeted by fraudsters to carry out a significant amount of APP scams.** The sectors represent 12% and 2% of the volume respectively and over 40% of the value.
- **Meta platforms were used by fraudsters to carry out more romance scams against UK payment users than all dating websites combined,** with 31% of romance scams being reported by consumers as starting on Meta platforms. (Facebook 14%, Instagram 10%, WhatsApp 7%). This constituted 22% of value.

[1] See page 10 for further details.

[2] The 14 largest banking groups in Great Britain and Northern Ireland were required to provide us with performance data under Specific Direction 18. You can find our reports for the last two years www.psr.org.uk/information-for-consumers/app-fraud-performance-data/

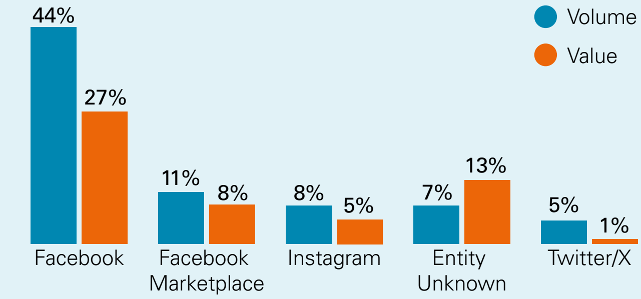
[3] Information gathering power under section 81 of the Financial Services (Banking Reform) Act 2013.

[4] APP scams performance report (July 2024).

[5] No firm level data is available for the Telecommunications and Email categories.

- **Meta platforms feature as the top three platforms being targeted by fraudsters to carry out the most common type of APP scam – purchase scams (by volume).** Facebook was used in 44% of incidents, Facebook Marketplace in 11%, and Instagram in 8%. Facebook was targeted by fraudsters to carry out the highest amount of losses at 27%. While eBay was used in only 1.6% of cases of purchase scams, it was used by fraudsters to carry out 9% of losses.

Purchase scams



- **Investment scams accounted for the highest proportion of losses**, at 24%, despite being just 6% of the volume of total APP scams. The telecommunication industry was used to carry out 23% of this value, Meta platforms 14% and families and friends 12%.

The benefits of publishing this data

Collecting and publishing this data supports our statutory objective that payment systems work in the interests of businesses and consumers who use them. The benefits of publishing this data are:

- **Raising consumer awareness and vigilance** by highlighting which platforms and services fraudsters most often exploit.
- **Improving the ecosystem's understanding of the scale of the threat.** We want firms to know how much fraudsters target victims to carry out APP scams. This should empower them to do more to prevent APP scams happening and encourage cross-industry collaboration.
- **Providing valuable insights for payment firms** to build risk profiles of fraudulent methodologies, based on their consumers' use of particular platforms and services. This should allow for better-targeted interventions.
- **Support other UK regulators like Ofcom and the government** to enforce duties and take actionable steps to prevent harm to society.

While we recognise and welcome initiatives from technology, telecommunications and social media firms and the payment industry to better understand the threats and improve their collective response, APP scams remain a major problem.

We consider that systemic action is needed to address the scale of the threat. Better data sharing and cross-industry collaboration can provide actionable data insights to support all sectors, public and private, to work together and make interventions earlier on in the fraud lifecycle. **We call on technology, telecommunication and social media platforms to work with payment firms to close down vulnerabilities that fraudsters exploit**. This will reduce harm and result in better outcomes for consumers.

We intend to publish this data every year and intend to consult in 2025 on how to improve data collation.

Scam types

The 14 largest banking groups in Great Britain and Northern Ireland provided scam incidents recorded against technology, telecommunication and social media platforms and services, broken into the following subcategories:

Laptop for sale
£999
Payment received

We haven't received payment for this item. Please send immediately.

I have already paid through the app.

Please send the money. I haven't had payment.

Purchase scams

The victim pays for a good or service that they do not receive and the seller had no intention of providing. The scammer may create a fake website or advertise a false product on social media.

My love, I must know many things about you.

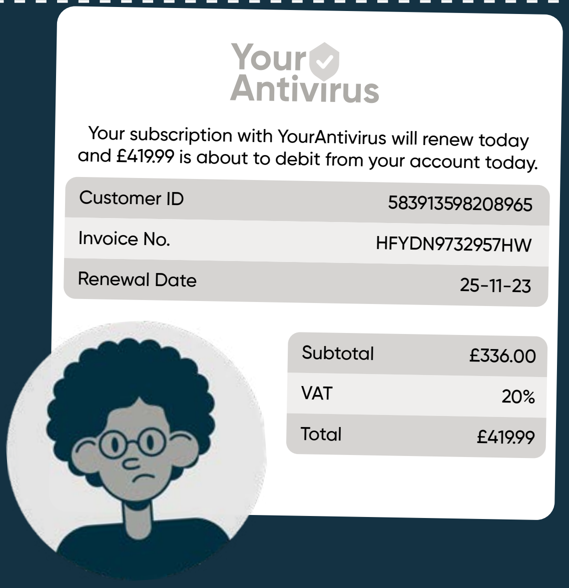
What is the name of your first pet?

What is your mother's maiden name?

What is the name of the town where you were born?

Romance fraud

The fraudster feigns a romantic interest in the victim to win their trust and manipulate them into sending money.



YourAntivirus

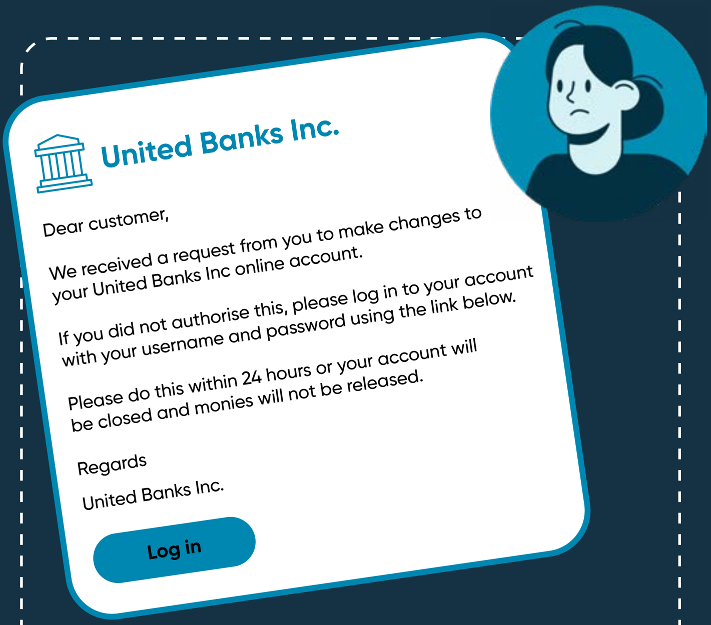
Your subscription with YourAntivirus will renew today and £419.99 is about to debit from your account today.

Customer ID	583913598208965
Invoice No.	HFYDN9732957HW
Renewal Date	25-11-23

Subtotal	£336.00
VAT	20%
Total	£419.99

Invoice and mandate fraud

The fraudster sends a fake invoice to the victim requesting payment for a good or service.



United Banks Inc.

Dear customer,

We received a request from you to make changes to your United Banks Inc online account.

If you did not authorise this, please log in to your account with your username and password using the link below.

Please do this within 24 hours or your account will be closed and monies will not be released.

Regards

United Banks Inc.

Impersonation scams

The fraudster pretends to be a law enforcement officer or bank staff to convince the victim to make a payment.

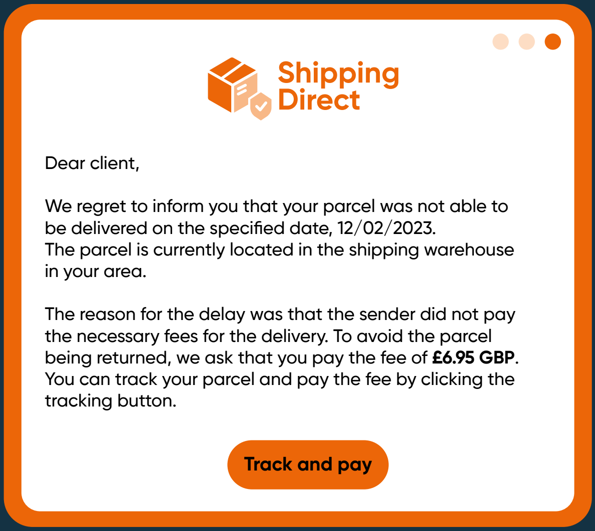
Your Friend

You must deposit a minimum of £1500.00

You must pay a withdrawal fee of £500.00

Investment fraud

The fraudster convinces the victim to invest in something that does not exist with the promise of a high return. The scammer may be pretending to be a financial advisor and using cold calling to reach out to the victim.



Shipping Direct

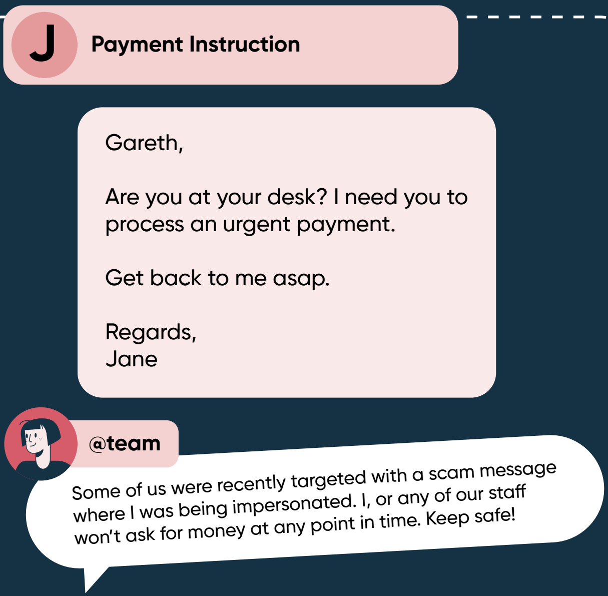
Dear client,

We regret to inform you that your parcel was not able to be delivered on the specified date, 12/02/2023.
The parcel is currently located in the shipping warehouse in your area.

The reason for the delay was that the sender did not pay the necessary fees for the delivery. To avoid the parcel being returned, we ask that you pay the fee of **£6.95 GBP**. You can track your parcel and pay the fee by clicking the tracking button.

Advance fee fraud

The fraudster convinces the victim to pay a fee which they claim will result in the release of a much larger payment or a deposit for goods or service that they never receive, and the fraudster never intended to provide.



J **Payment Instruction**

Gareth,

Are you at your desk? I need you to process an urgent payment.

Get back to me asap.

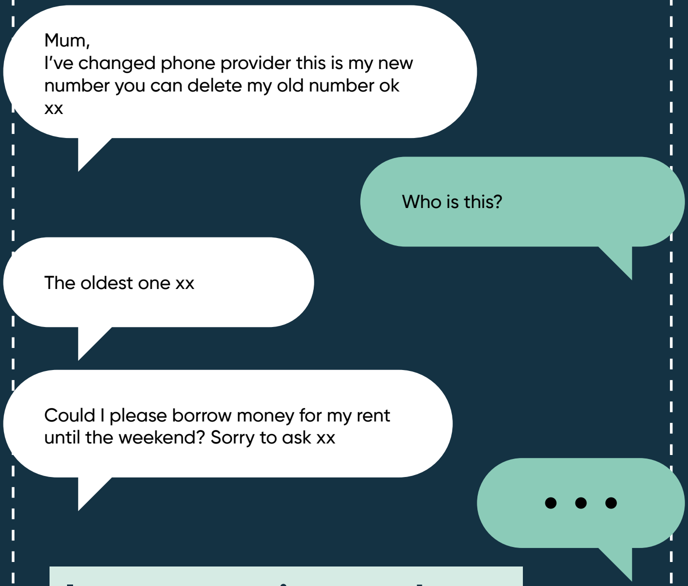
Regards,
Jane

@team

Some of us were recently targeted with a scam message where I was being impersonated. I, or any of our staff won't ask for money at any point in time. Keep safe!

Impersonation – CEO

The fraudster pretends to be a CEO or other workplace figure to convince the victim (often employees of a business) to make a payment.



Mum,
I've changed phone provider this is my new number you can delete my old number ok
xx

Who is this?

The oldest one xx

Could I please borrow money for my rent until the weekend? Sorry to ask xx

• • •

Impersonation – other

The fraudster pretends to be someone, commonly family or friends, or a celebrity or public figure to convince the victim to make a payment.

Introduction

An APP scam is where a person dishonestly manipulates, deceives or persuades a consumer into transferring funds from the consumer's account to an account outside of their control, where:

- the recipient is not who the victim intended to pay, or
- the payment is not for the purpose intended.

APP scams can be complex and involve multiple actors. These can include payment firms – who operate the facilities where money loss occurs – and technology, telecommunication and social media platforms – which fraudsters use to communicate with victims and persuade them to make payments.

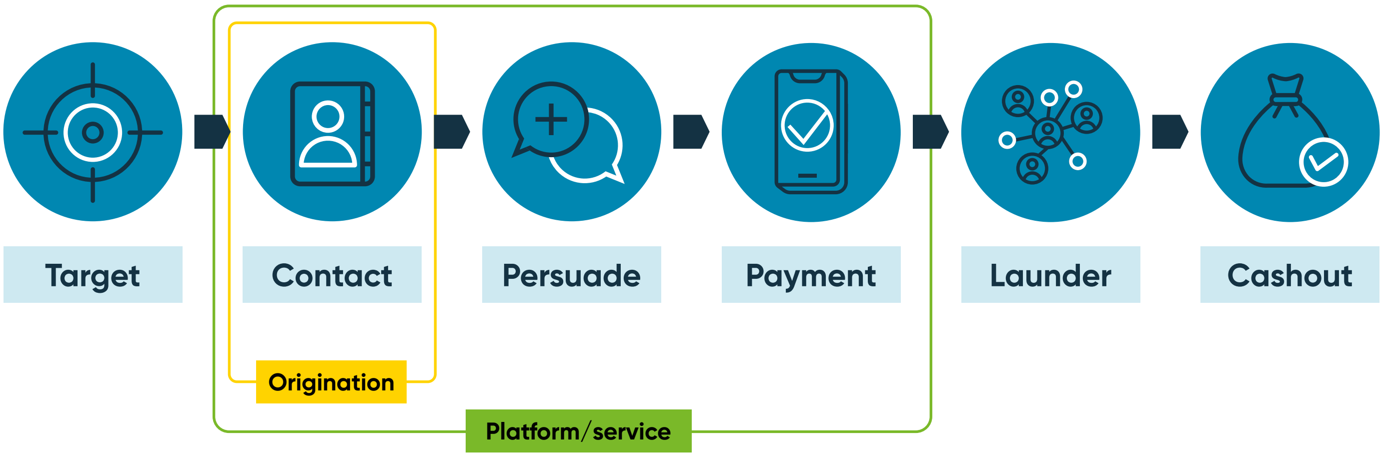
How fraudsters abuse legitimate platforms

Scams occur when criminals exploit legitimate services and systems to make false representations with the intention to make a gain, or cause a loss, or the risk of a loss, to another. This includes payment firms, agents or other entities whose systems are exploited to carry out fraud. We have previously published performance data on payment firms. For the purpose of this data publication, we defined an entity used to carry out APP scams as either:

- A platform or service through which the fraudster made contact with the victim; or
- A platform or service where the victim saw an advertisement or profile that subsequently results in an APP scam.

How do scams occur?

APP scams vary, but most follow a pattern of:



Targeting the victim (for example, using stolen data, finding vulnerable target groups on social media, or creating false advertisements)

Contacting the victim (for example, through adverts, direct messages, phone calls, text messages)

Persuading the victim to make a payment

Laundering the money and cashing out

Case study

A social media account belonging to a friend of a victim posted about good returns on an investment, highlighting the 'benefits of crypto investments'. The victim was gradually coached into transferring over £2,000 into an alleged cryptocurrency scheme. When the victim wanted to withdraw their money, they were charged fees, which they paid. After further demands were made, the victim realised they had been defrauded and later found out their friend's account had been hacked.

OMG – you don't want to miss this investment opportunity. I have made over 70k and it's changed my life!!! Such good returns at 5% and celebrities use it!

2 March

Victim
I am really interested and have never done this. What do I do? How much should I put in?

Fraudster
Hi there – you need to register here. Its really easy and you can watch your investments grow on the dashboard. If you have any questions, just reach out. I am here to help 😃.

Maybe start with £500. You can then watch the money roll in!

29 March

Fraudster
Hi there – I just wanted to see how your investment was going? Is there anything I can do to help?

Victim
Hi – Its going well, I can't believe my investment has already started to grow over the last month.

Fraudster
That's great. If you're happy with the way things are going, do you want to invest more?

Victim
Yeah I'll put in another £500!

Fraudster
Are you sure? I know other people are seeing really big returns at the moment. I would hate for you to miss out. I would recommend putting in 2K.

Victim
Ok I'll do that.

30 June

Victim
Hi, I have been happy with my investments and want to withdraw some of my money, but it says I have to pay fees, which I have done, its now asking for more?

Fraudster
Yes, that's an admin fee, everyone has to pay. Without it your money can't be released.

Victim
Hello it is asking for more...

Victim
Why are you not responding? I want my money!

The transcript has been generated from a victim's experience and testimonial.

How do APP scams impact victims and trust in payments and institutions?

We are concerned by the threat that APP scams pose to trust in payment systems and consumer confidence. We therefore commissioned Thinks Insight to produce a study on how APP scams affect victims' confidence in payments and other economic activities.

Of the 688 victims surveyed:

32% of victims reported they are less willing to try new payment methods.

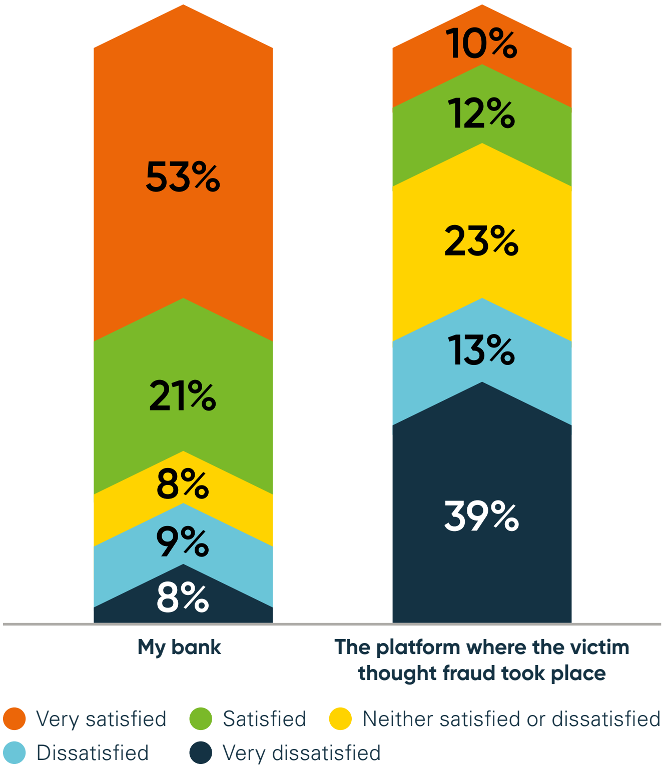
36% of victims were less likely to try new approaches to managing their finances because of their experience.

48% reported they were less likely to shop with a new retailer they haven't heard of before.

The study also showed that victims thought technology companies were in part responsible – alongside their bank, the fraudster, and the police. Furthermore, only 22% were satisfied with the response of technology companies, compared to 74% for banks. 41% said they had lost trust in social media – four times as many as had lost confidence in banks.

You can find the full study here.

Levels of victim satisfaction with banks versus platforms and services



Data collection

The data we have collected is reported by victims. When people become victims of fraud, they are more likely to report the incident to their bank than to the police. Payment firms have started logging when victims report that a social media platform, telecommunication or technology firm was used in the scam. This has created a rich dataset of which platforms and services are most commonly targeted by fraudsters to carry out APP scams. While efforts are made by payments firms to ensure the accuracy of the data, human error by the case handler can impact the data quality. In addition, our data shows that in some cases, the victim may not remember where the initial compromise happened. In other cases, the consumer may report in error where they believe a scam originated, when in fact the fraudster made contact with them earlier and on another platform. We intend to consult on how we can improve data collection in the future. You can find more detail on how this data is gathered on pages 22 to 23.

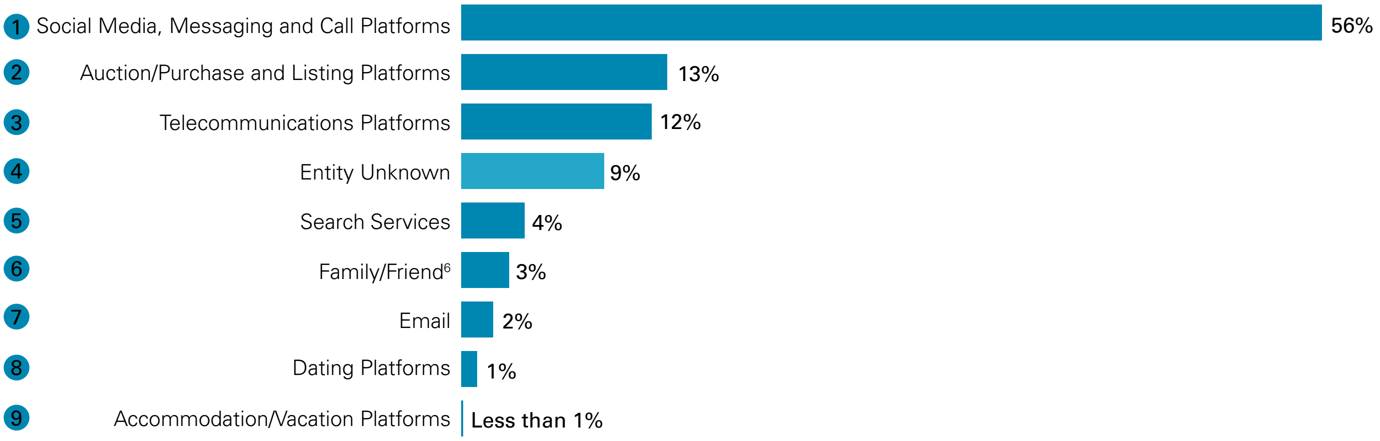
APP scam reported by sector in 2023

In 2023, social media platforms were targeted by fraudsters to carry out 56% of the volume of APP scams (124,057 incidents) and 20% of the value lost (£67,429,184), while auction/purchase and listing platforms were targeted by fraudsters to carry out 13% of cases (29,473 incidents) and 6% of losses (£21,283,030).

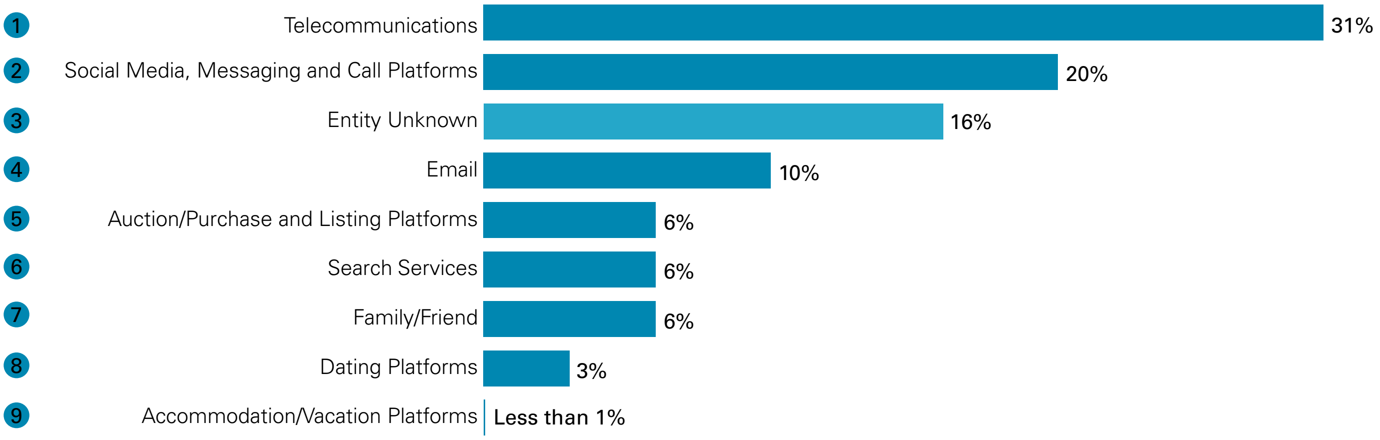
Telecommunications platforms were targeted by fraudsters to carry out a significant amount of APP scams via fraudulent calls and text messages, at 12% of volume (26,975 incidents) and 31% of value lost (£107,229,381). Email providers were also targeted by fraudsters to carry out disproportionality high losses at 10% by value (£35,001,770) but only 2% of the volume (3,955 incidents).

Data recorded by payments firms does not currently break down telecommunication and email data by individual provider level. We intend to consult on how this data collection can be improved in 2025.

Scam by sector (ranked by volume)



Scam by sector (ranked by value)



[6] This includes data where the scam included family or friends of the victim.

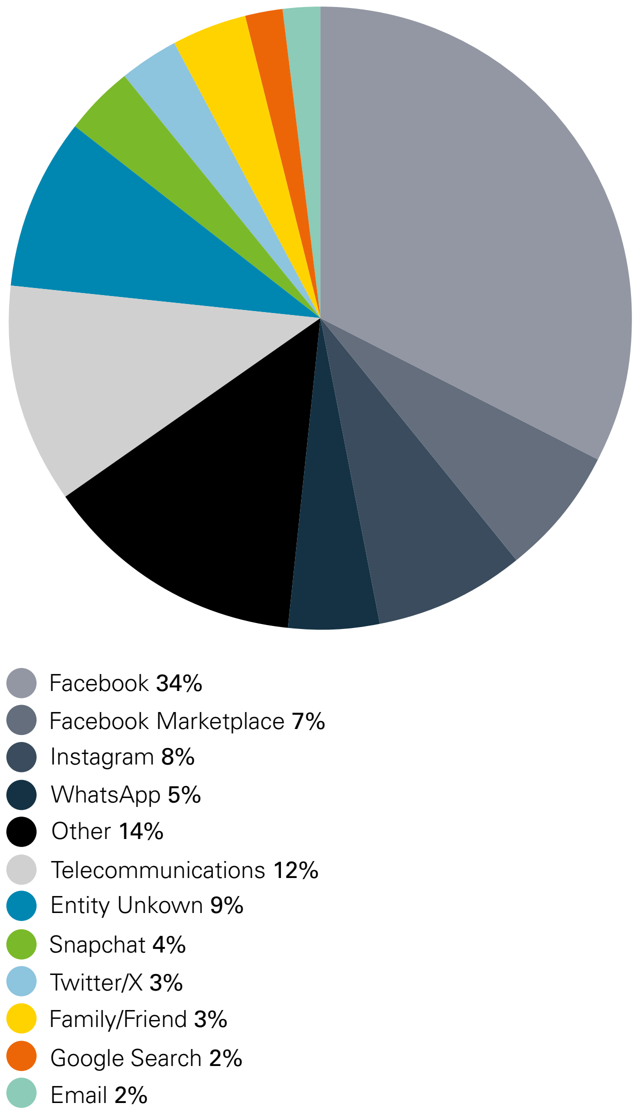
Data notes: The figures have been rounded up or down and may not equate to 100% across volume and value totals.

The most common platforms and services used by fraudsters

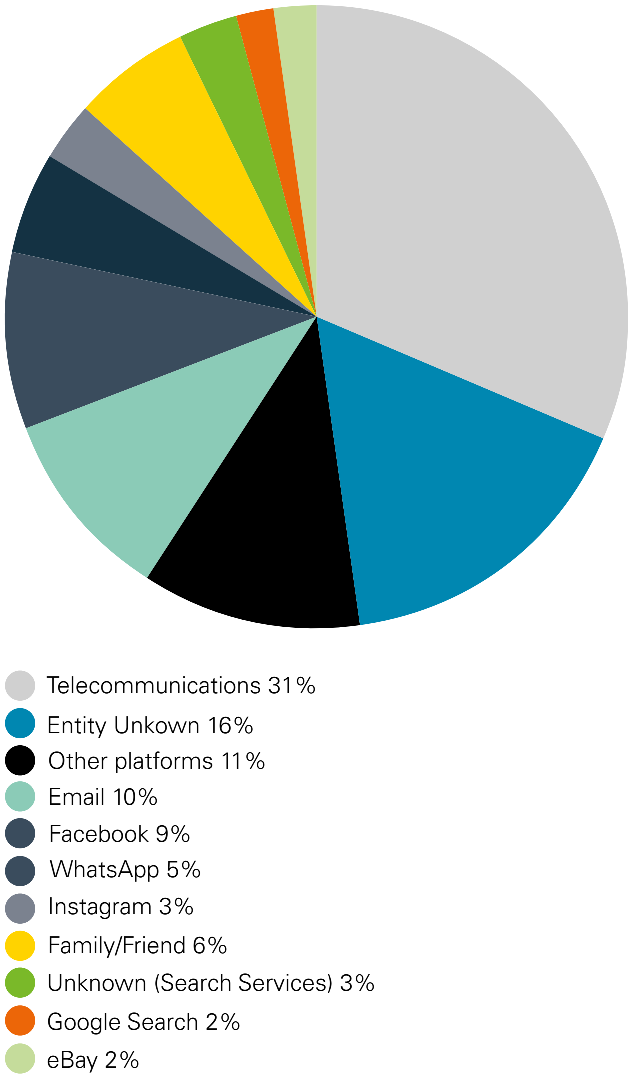
Over half of all APP scams recorded in 2023 were reported by victims as originating on Meta platforms. Meta platforms were recorded as being targeted by fraudsters to carry out 54% of volume (119,338 incidents) and 18% by value (£62,691,418). This means Meta platforms were used by fraudsters to carry out the loss of approximately £1 in every £5 lost in an APP scam.

The telecommunications sector was targeted to carry out 12% of APP scams by volume (26,975 incidents) and 31.5% by value (£107,229,381).

Most common entities used by fraudsters (by volume)



Most common entities used by fraudsters (by value)



Data notes: The figures have been rounded up or down and may not equate to 100% across volume and value totals.

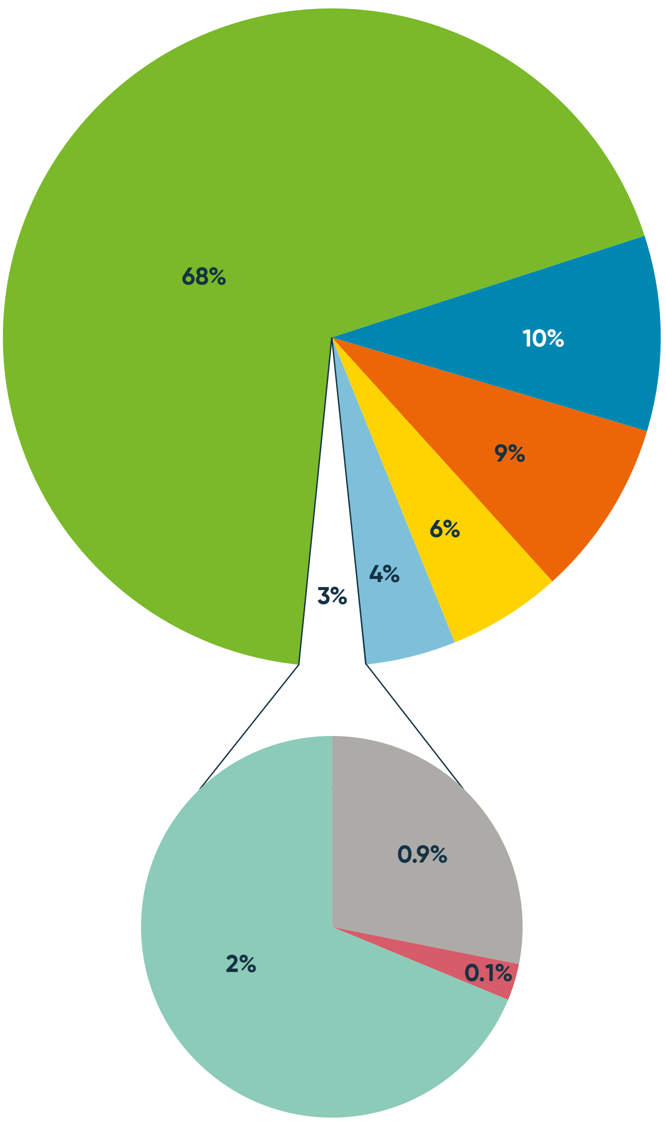
Scams type – overview

Purchase scams are the most common type of APP scams in the UK, making up 68% of cases in 2023 (152,192 incidents). Impersonation scams combined make up 14% (31,321 incidents) and advance fee scams, the third most common, made up 9% with 19,341 incidents.

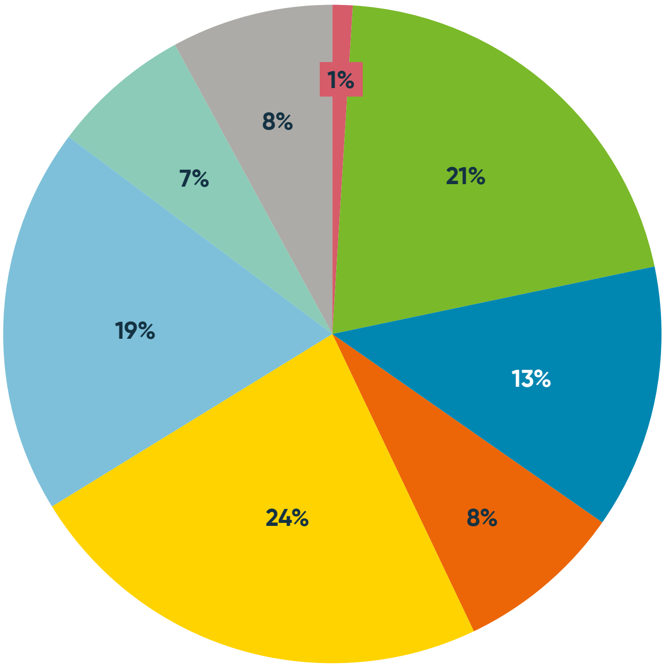
Impersonation scams combined made up 33% of losses (£107,061,348). Investment scams make up 24% of losses (£80,276,625) despite accounting for only 6% of volume (12,500 incidents). Purchase scams made up 21% of losses (£72,403,187).

- ● Purchase Scam
- ● Advance Fee Scam
- ● Romance Scam
- ● CEO Scam
- ● Impersonation Scam – Other
- ● Investment Scam
- ● Invoice and Mandate Scam
- ● Impersonation Scam – Police/ Bank Staff

Volume of fraud by scam type



Value of losses by scam type



Purchase scams (highest ten)

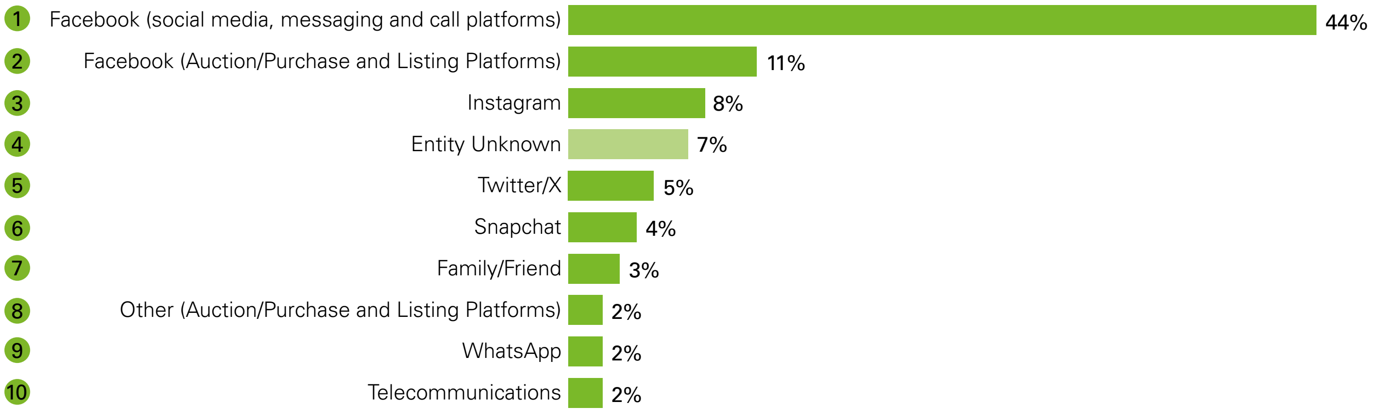
In purchase scams, the victim pays for a good or service that they do not receive and the seller had no intention of providing. The scammer may, for example, create a fake website and promote it through search services or spam, advertise a fake product on social media, or create a fake listing on an auction website.

Meta platforms feature as the top three firms most commonly targeted by fraudsters to carry out purchase scams, by volume. Facebook was used in 44% of incidents in 2023 (67,337), Facebook Marketplace in 11% (16,067 incidents), and Instagram in 8% (11,885 incidents).

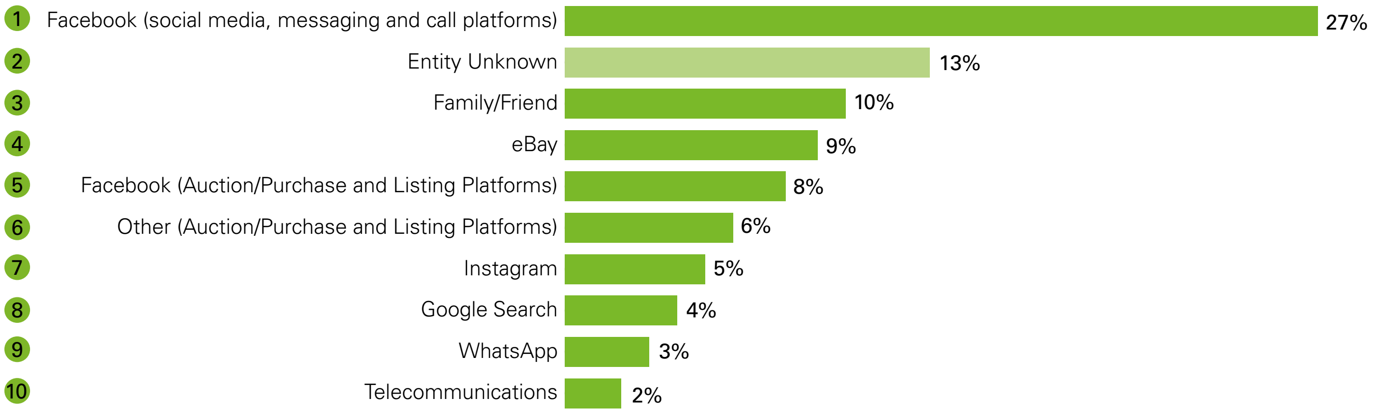
Twitter/X was targeted to carry out 5% of purchase scams (7,096 incidents) and Snapchat 4% (6,359 incidents).

Facebook was used by fraudsters to carry out the most scams by value, at 27% of the total (£19,509,964). While eBay only accounted for 1.6% of volume (2,370 incidents)[7], its platform was used by fraudsters to carry out 9% of losses (£6,659,382).

Purchase scams: most common entities (ranked by volume)



Purchase scams: most common entities (ranked by value)



[7] Ebay falls outside of highest 10 for volume.

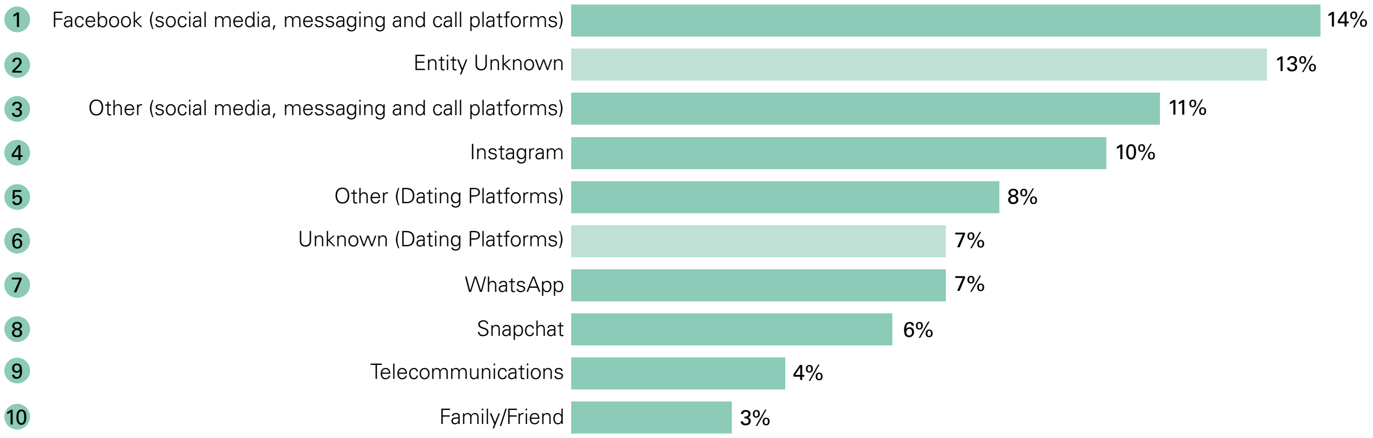
Romance scams (highest ten)

A romance scam is when a fraudster feigns a romantic interest in the victim to win their trust and manipulate them into sending money. Romance scams are less common, with 4,997 incidents in the UK in 2023, but they can be financially and emotionally devastating.

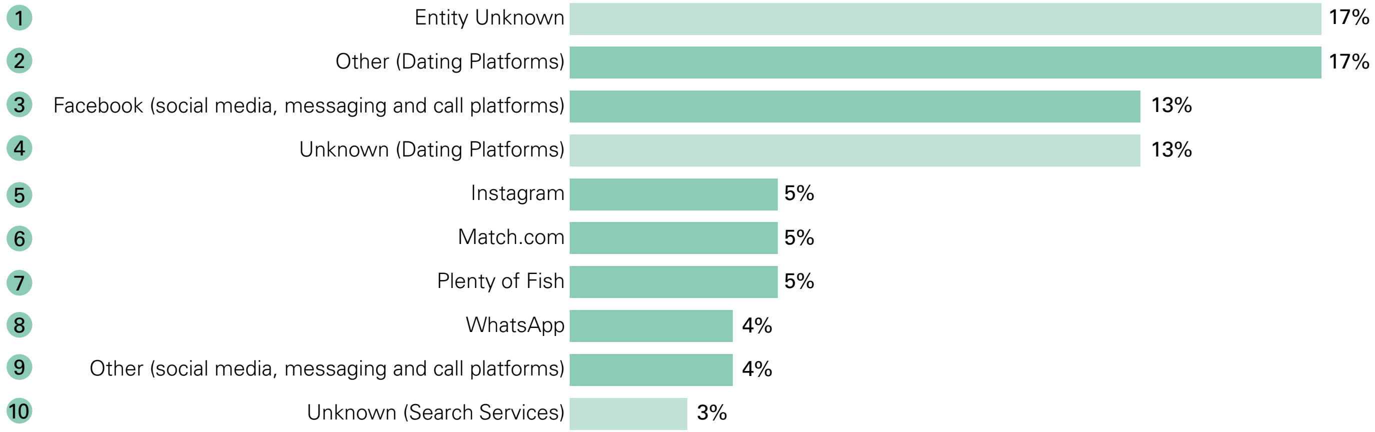
Meta platforms were used by fraudsters to carry out more romance scams against UK payment users than all dating platforms combined, with 31% of the volume (1,590 incidents). Facebook accounted for 14% of the total (719 incidents), Instagram 10% (511 incidents), and WhatsApp 7% (360 incidents). This made up 22% of the total value lost (£5,072,115).

In 13% (662 incidents) of cases the party was not known, accounting for 17% of losses (£3,900,035). There are many reasons for this: a victim may not be able to remember, or in some cases may not want to reveal how the fraudster contacted them. We intend to consult on how we can improve data collection in the future.

Romance scams: most common entities (ranked by volume)



Romance scams: most common entities (ranked by value)



Investment scams (highest ten)

In investment scams, the fraudster convinces the victim to invest in something that does not exist with the promise of a high return.

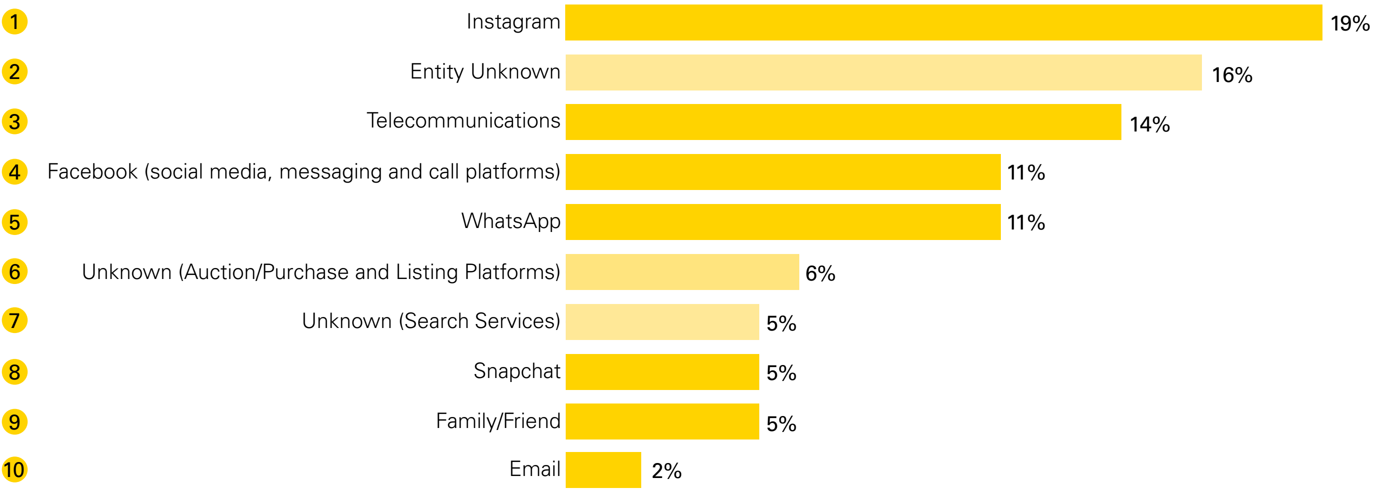
Investment scams account for the greatest losses of all APP scams, at 24% of the 2023 total (£80,276,625), despite being only 6% of the volume (12,500 incidents).

Of these investment scams, Meta platforms were used to carry out 41% of incidents and 14% of losses: 19% (2,418) of incidents occurred through Instagram, 11% (1,402) through Facebook, and 11% (1,314) through WhatsApp.

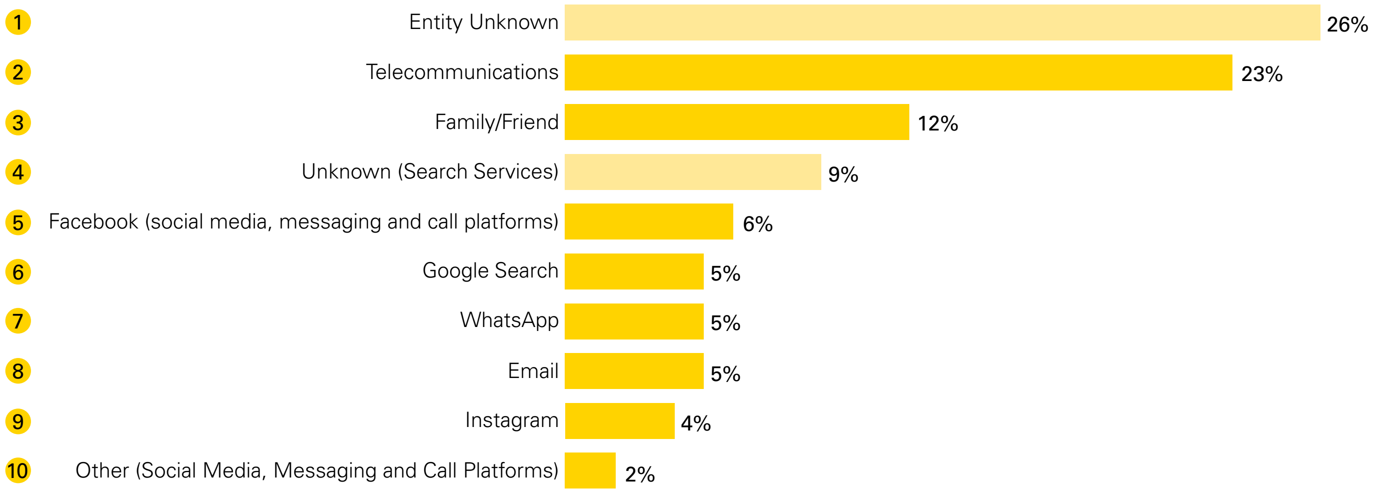
In 16% (1,960) of incidents in 2023 the entity was not known, accounting for 26% of losses (£20,533,462). We intend to consult on how we can improve data collection in the future.

Telecommunications companies were used to carry out 14% of the total volume (1,694 incidents) and 23% of losses (£18,396,441).

Investment scam entities (ranked by volume)



Investment scams: most common entities (ranked by value)



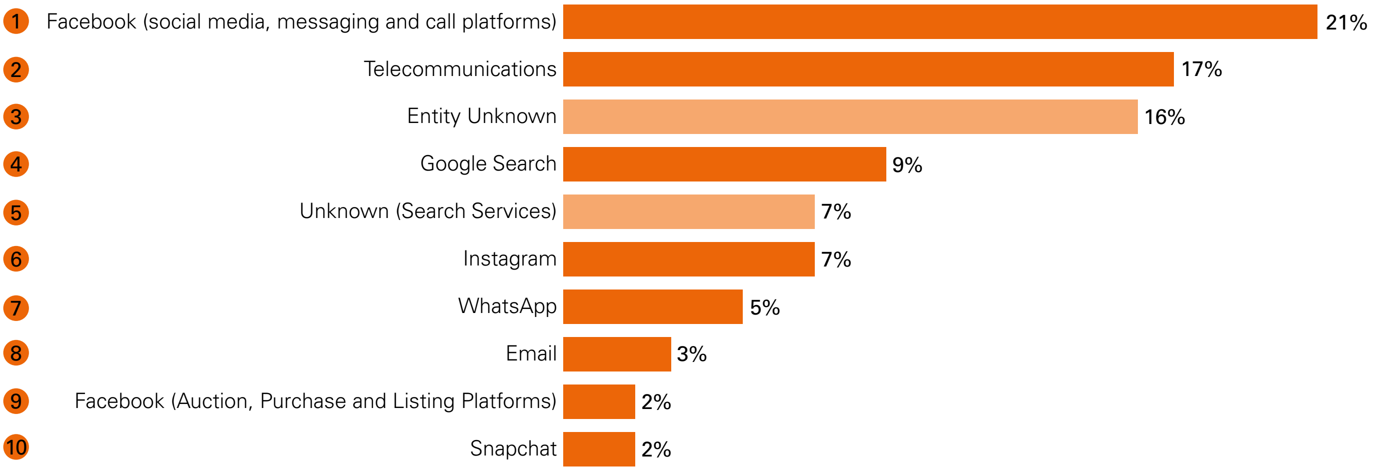
Advance fee scams (highest ten)

In advance fee scams, the fraudster convinces the victim to pay a fee which they claim will result in the release of a much larger payment or a deposit for goods or service that they never receive, and the fraudster never intended to provide. This can include claims that the victim has won a holiday, is entitled to an inheritance or is awaiting the delivery of goods.

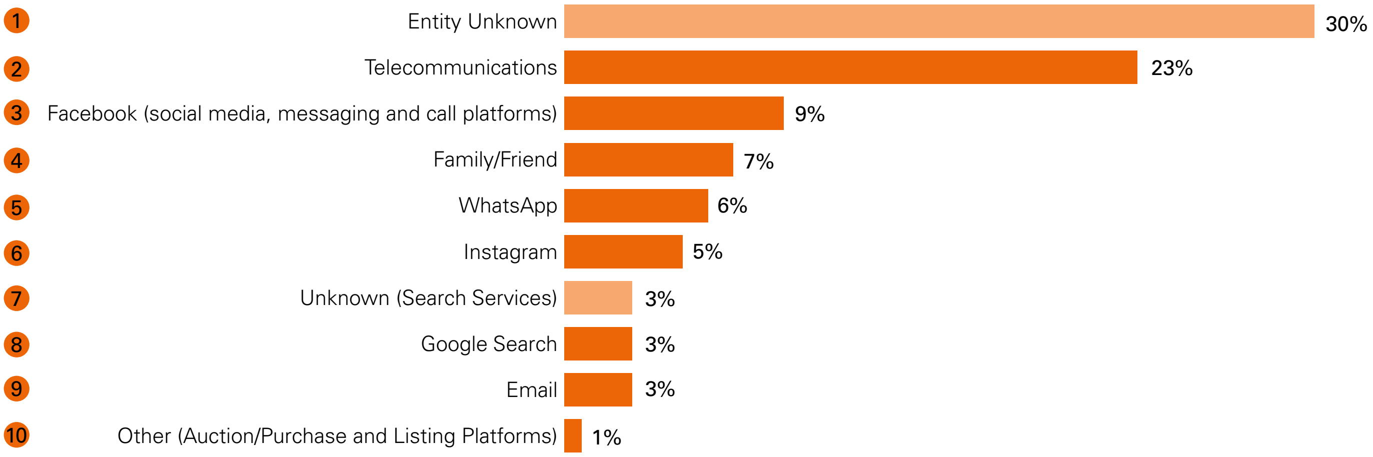
Advance fee scams made up 9% (19,341) of APP scams by volume in 2023. Fraudsters most commonly used Facebook, with 21% of the total cases (4,035). This was followed by telecommunication companies, at 17% of volume (3,234), and the third most common category in our data is 'unknown' at 16% of cases (3,181).

Cases with an unknown entity accounted for the most value lost, with 30% of the total (£7,852,261). Where the entity was known, losses were highest when they occurred via telecommunication (23%, £5,904,924) followed by Facebook (9%, £2,390,578) and friends and family (7%, £1,828,793).

Advance fee scams: most common entities (ranked by volume)



Advance fee scams: most common entities (ranked by value)

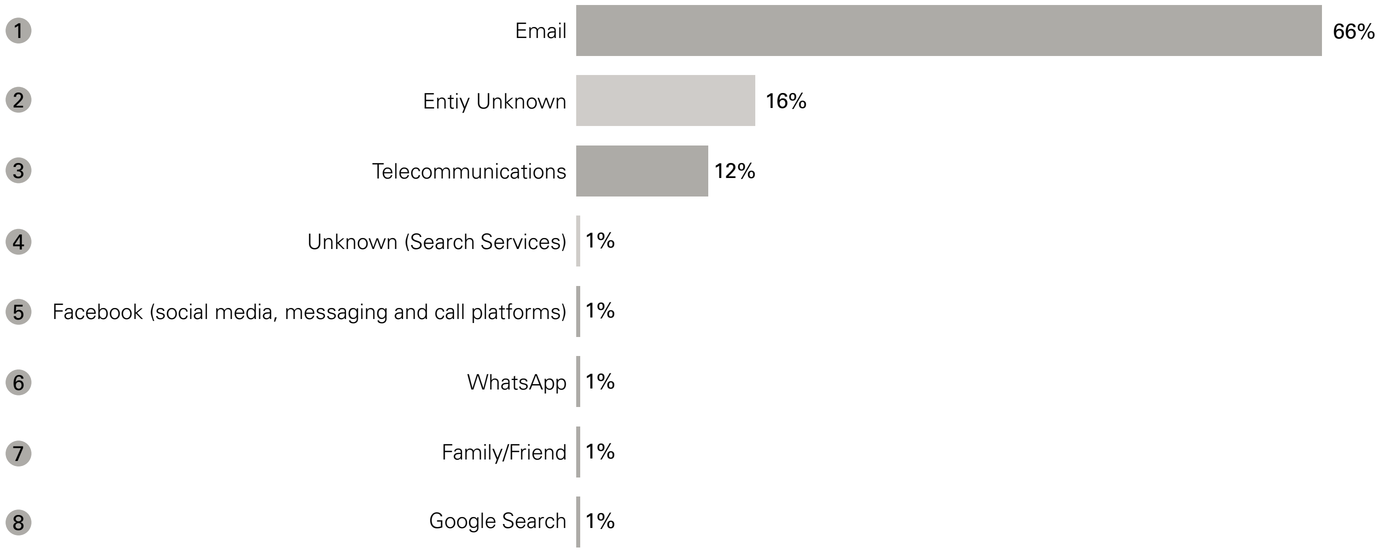


Invoice and mandate scams (highest ten)

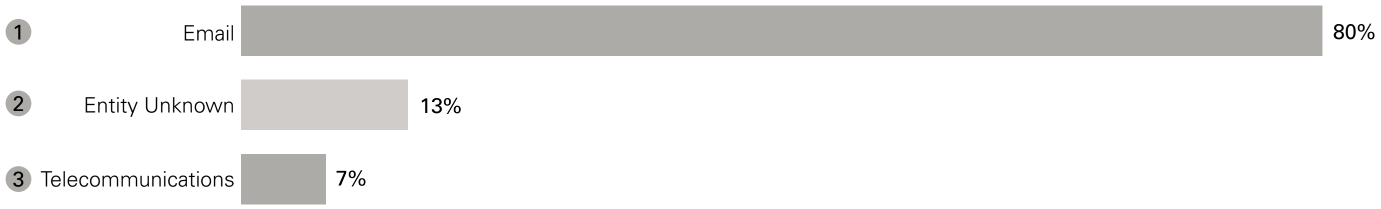
In invoice and mandate scams, the fraudster sends a fake invoice to a victim. This is often perpetrated against businesses through email, with 66% of the total volume in 2023 (1,301) and 80% of the value (£22,639,756) occurring in this way.

In 16% of cases (317 incidents) the entity could not be identified, accounting for 13% of value lost (£3,568,494). 12% of cases occurred over the phone (235 incidents), which accounted for 7% of the value lost (£2,048,205).

Invoice and mandate scams: most common entities (ranked by volume)



Invoice and mandate scams: most common entities (ranked by value)



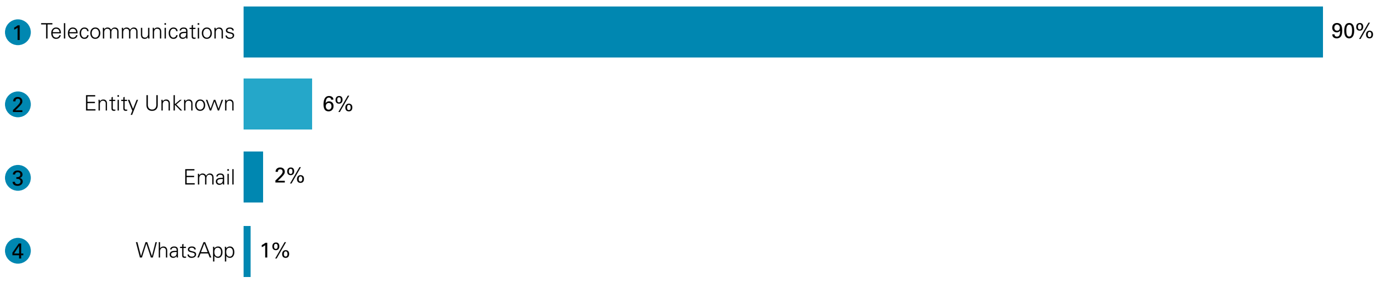
Data notes: The volume and value charts have fewer than ten platforms shown because some of the categories/subcategories have figures close to 0% and have been omitted on this basis from the chart. Data on those firms can be found in the data tables.

Impersonation scams – police and bank staff (highest ten)

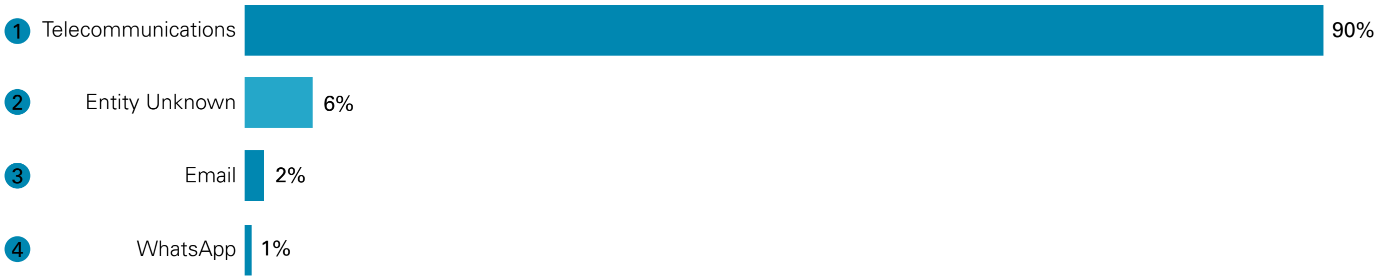
In impersonation scams, the fraudster pretends to be someone known to the victim, or someone in a position of authority or trust. This is a high-harm scam type because victims can experience high levels of long-lasting stress and emotional harm. In some cases, victims can lose their entire savings and there is permanent loss of trust in institutions and payments.

Police and bank staff impersonation scams are largely perpetrated via telecommunication, with 90% of cases in 2023 (8,990 incidents) occurring via text or phone call. In this type of scam, fraudsters often want victims to clear their entire bank account, so the losses are very high, with £57,719,548 lost through telecommunication alone.

Impersonation scams (police/bank staff): most common entities (ranked by volume)



Impersonation scams (police/bank staff): most common entities (ranked by value)



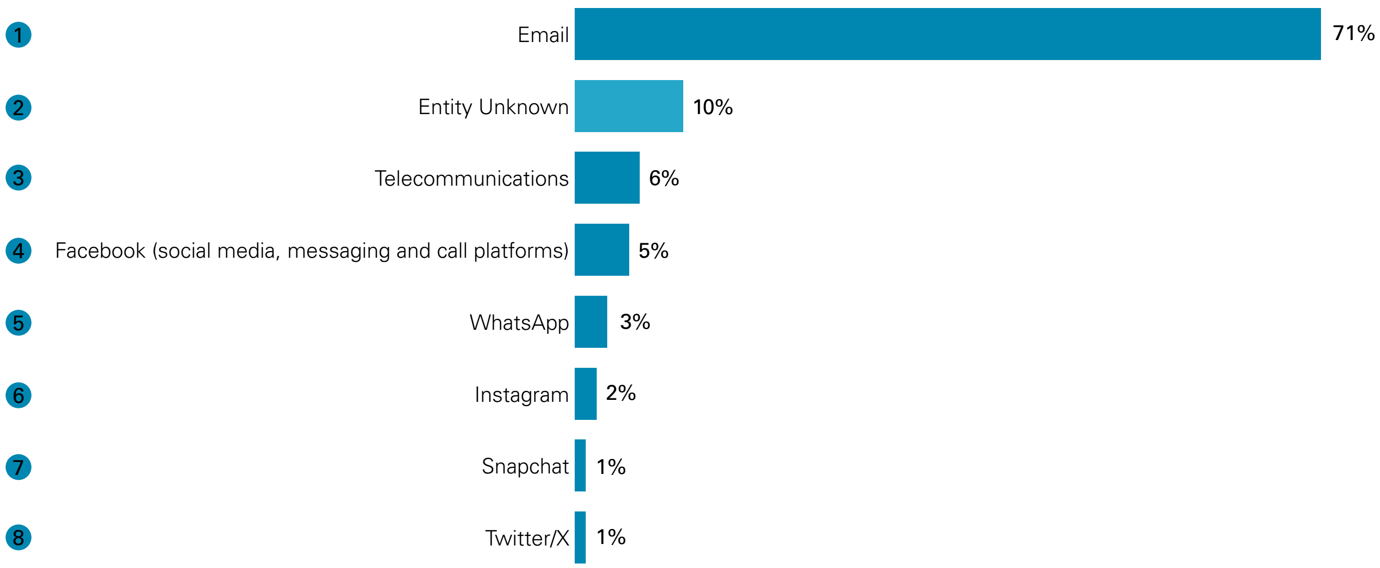
Data notes: The volume and value charts have fewer than ten platforms shown because some of the categories/subcategories have figures close to 0% and have been omitted on this basis from the chart. Data on those firms can be found in the data tables.

Impersonation scams – CEO (highest ten)

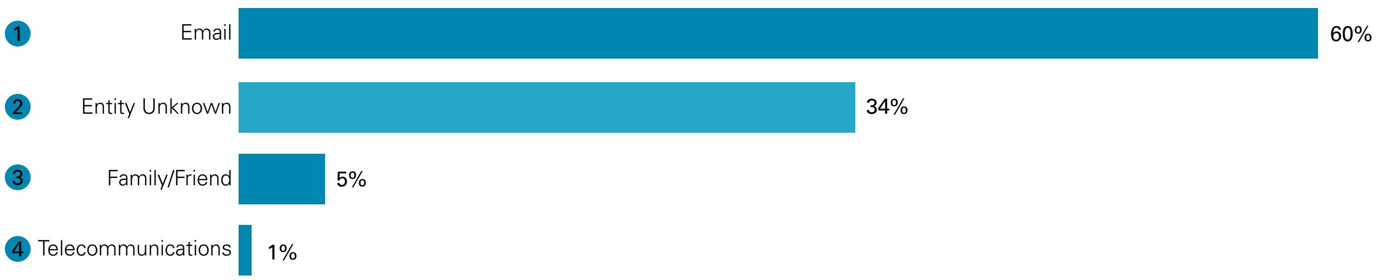
CEO scams are a type of scam where someone impersonates a senior figure in a workplace to trick staff into making payments.

It is largely perpetrated through email, with 71% of cases in 2023 (153 incidents) occurring in this way. This accounted for 60% of the value lost (£2,297,287). Fraudsters commonly target businesses in this scam.

Impersonation scams (CEO): most common entities (ranked by volume)



Impersonation scams (CEO): most common entities (ranked by value)

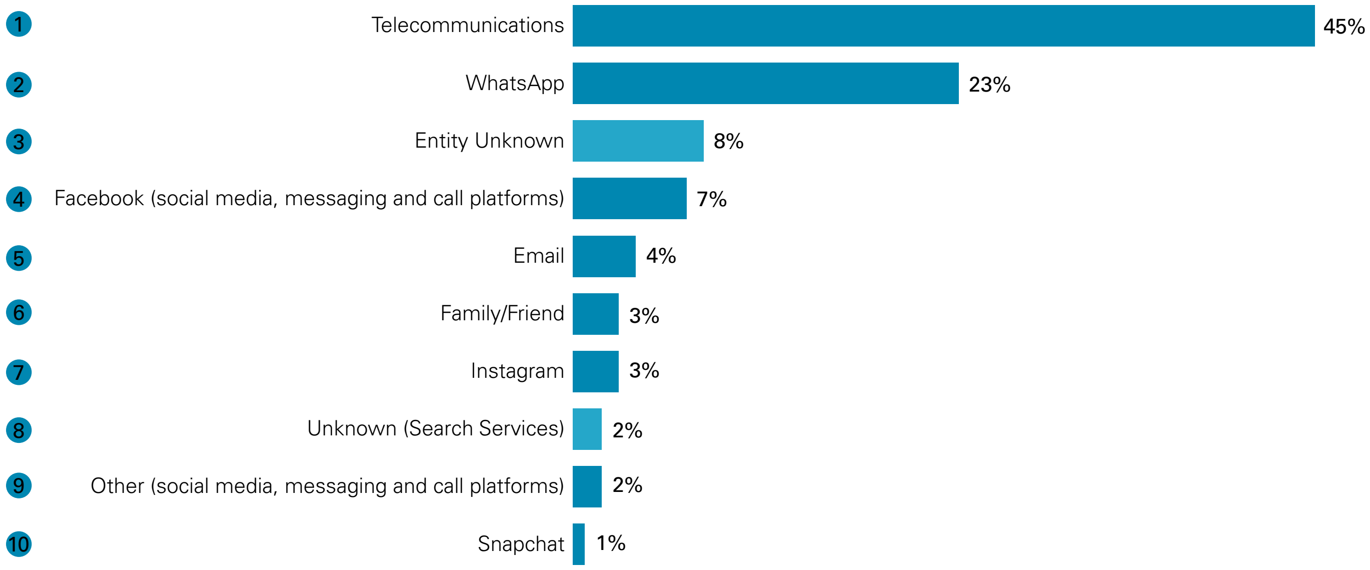


Data notes: The volume and value charts have fewer than ten platforms shown because some of the categories/subcategories have figures close to 0% and have been omitted on this basis from the chart. Data on those firms can be found in the data tables.

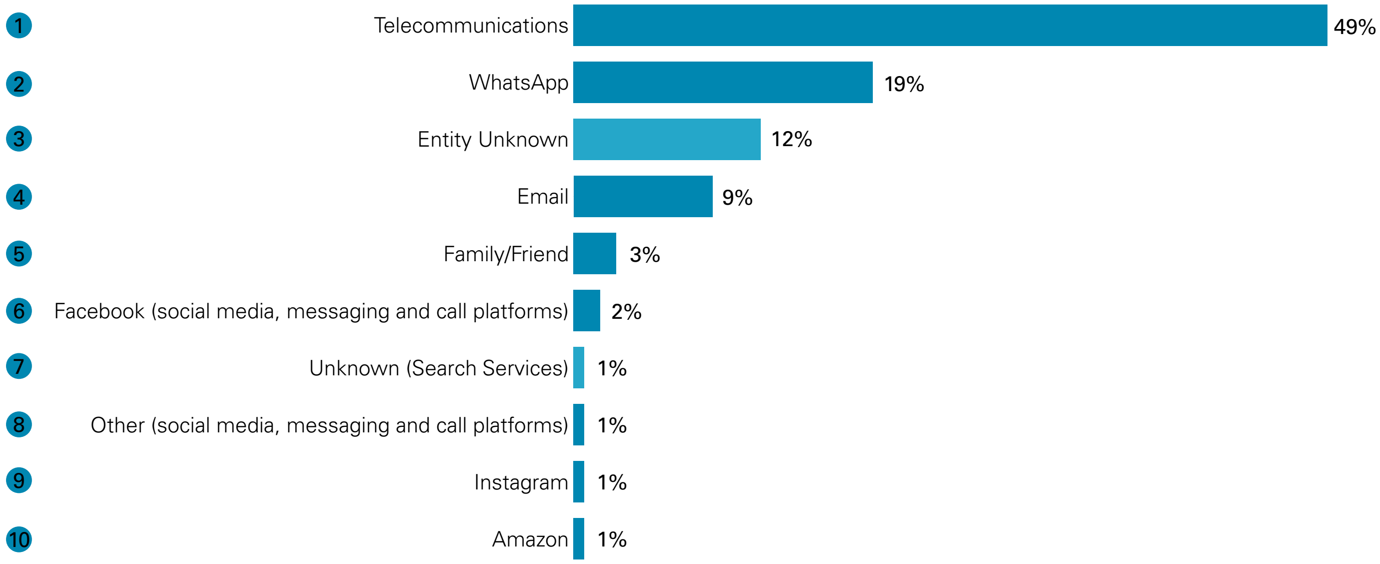
Impersonation scams – other (highest ten)

Other impersonations scams – including friends and family impersonation – happen commonly via telecommunication, accounting for 45% of total cases and 49% of total value in 2023 (9,529 incidents, for £20,941,262). This is followed by WhatsApp at 23% of cases, with 4,993 incidents and £8,238,709 lost (19% of total value).

Impersonation scams (other): most common entities (ranked by volume)



Impersonation scams (other): most common entities (ranked by value)



Data notes: In some of these impersonation cases, a fraudster may have deceived a victim into thinking that they are staff of a given platform or service. It may be that the scam did not originate on the platform or service it has been attributed to, but the name of the platform or service was used by the fraudster to trick the victim.

How was this data gathered?

We requested data from the 14 largest payment service providers (PSPs) in Great Britain and Northern Ireland, who together account for the majority of UK retail banking transactions. We also require these firms to provide us with regular APP scam performance data. They are:

Allied Irish Bank (AIB) Group
Barclays Bank UK plc
The Co-operative Bank plc
HSBC UK Bank plc
Lloyds Bank plc
Metro Bank plc
Monzo Bank Limited
National Westminster Bank plc
Nationwide Building Society
Northern Bank Limited (trading as Danske Bank)
Santander UK plc
Starling Bank Limited
TSB Bank plc
Virgin Money UK plc

We requested APP scams data on the organisations below, where the platform or service was recorded at least once as used by fraudsters to carry out APP scams across the different scam types. Not all the firms listed were recorded across all scam types. The charts between pages 14 to 21 and data on pages 28 and 29 only contain the rankings and data of the highest ten platforms or services.

Email providers	No company-level data available
Social media, call and messaging platforms or apps	LinkedIn, Twitter/X, Snapchat, Telegram, Facebook, Instagram, WhatsApp, Unknown, Other
Accommodation/ vacation website or app	SpareRoom, Airbnb, Unknown, Other
Entity Unknown	
Auction/purchase and listing platforms or apps	eBay, Gumtree, Amazon, Shpock, Pets4Homes, Facebook Marketplace, Unknown, Other
Telecommunications – no company-level data available	No company-level data available
Dating website or app	Tinder, Bumble, eHarmony, Hinge, Match.com, Plenty of Fish, Unknown, Other
Family/Friend	
Search services	Google Search, Bing, Yahoo, Ecosia, Unknown, Other

We requested data for all push payment types. The data in this report aggregates all these:

- Faster payments
- CHAPS
- Intra Bank Transfers
- Bacs payment
- Bacs Standing Order
- International SWIFT

We also asked for a breakdown of scams into the following subcategories:

- Purchase
- Romance
- Investment
- Advance fee
- Invoice and mandate fraud
- Impersonation – police/bank staff
- Impersonation – CEO
- Impersonation – Other

Data notes

1. The data we collected was victim self-reported i.e., when the victim reports to their payment firm where they believe the scam started. Noting that:

   a) In some cases, the victim may not remember where the initial compromise happened.

   b) In other cases, the consumer may report to their payment firm that a scam started on a specific platform, when in fact the fraudster made contact with them earlier and on another platform or service. For example, a victim may tell their payment firm that they believe the fraudster persuaded them to make a payment over telecommunication, but the point of original contact between the victim and fraudster was on a dating platform or via social media.

2. While all efforts were made by payment firms to ensure the accuracy of the data, the data may contain inputting errors by the case handler or subject to differences in interpretation by payments firms with assigning scams to platforms and services.

3. The payment firms we requested data from are members of UK Finance and participants of the Best Practice Standard (BPS) claims management platform. The BPS allows payment firms to create cases in real time, quickly passing information to other financial institutions whose customers may have received fraudulent money into their account. The real time nature of the platform greatly increases the chance of being able to stop the funds ending up in criminal hands.

4. Firms subject to the request were permitted to provide this data from their internal datasets or from BPS, so long as they used the format we specified and provided all the available data.

5. Most payment firms provided their data via BPS while some used a combination of BPS and their internal case management systems.

6. Participants of the BPS platform own the data entered and stored and are responsible for its accuracy and completeness. However, extensive testing, engagement with payment firms during the development of the platform, and validation with other sources of scam data have shown that the data from BPS is broadly consistent with industry trends.

7. As a claims management platform, the data inputted into BPS covers both confirmed and suspect fraud. For this exercise, we have only used data drawn from confirmed fraud cases which have been fully investigated and closed. Therefore, it is likely that not all incidents of scams will have been included in our data reporting.

8. The data inputted into the BPS platform relies on victims reporting to their payment firm. The total volume and value of fraud across the UK will then be higher than the numbers detailed here. BPS data may also be subject to future restatement if further information becomes available.

9. Once we received the data, we collated and analysed it and created a dataset for each individual entity and sector.

10. We have used data from firms and the industry body UK Finance to support the data described in our report.

11. There are minor differences for some scam types in comparison with UK Finance data. This is likely due to the limitation of our data being collected from 14 firms, whereas UK Finance data includes a wider set of payment firms. The more significant difference for the telecommunications and social media sectors is due to our categorisation of WhatsApp as a social media, messaging and call platform, whereas industry categorises it as telecoms.

12. We are aware that there are a small number of irregularities in how some scam cases have been allocated as originating on specific platforms. These irregularities may include inconsistencies between payment firms in the number of scams reported per platform, or as unexpected categorisation of scams into types not typically associated with a platform. This is likely to result from differing approaches and interpretation by payment firms at the time of recording the scam case and the victim's recollection of where the scam started.

How do scam type rankings work?

- The rankings presented in this report are based on the 40 categories and subcategories listed.
- Where firm level data is available, sector totals have been excluded from the rankings.
- This data was collected by payment firm and based on consumer reports, at the time of when a victim reports a scam. Therefore:
  - If a consumer did not know, did not remember, or did not want to reveal which sector the fraudster contacted them on, the payment firm staff marked it as 'Entity unknown'.
  - If the consumer revealed the sector but not the platform, then the payment firm marked the entity as 'Unknown (Sector Name)'.
  - If the consumer revealed the sector but the platform is not listed in the entity list used by the payment firm staff, then the payment firm marked the entity as 'Other (Sector Name)'.

List of categories/sub-categories to be ranked
Airbnb
Amazon
Bing
Bumble
eBay
Ecosia
eHarmony
Email
Entity unknown
Facebook (Auction/Purchase and Listing Platforms)
Facebook (Social Media, Messaging and Call Platforms)
Family/Friend
Firefox
Google Search
Gumtree
Hinge
Instagram
LinkedIn
Match.com
Other (Accommodation/Vacation Platforms)
Other (Auction/Purchase and Listing Platforms)
Other (Dating Platforms)
Other (Search Services)
Other (Social Media, Messaging and Call Platforms)
Pets4Homes
Plenty of Fish
Shpock
Snapchat
SpareRoom
Telecommunications
Telegram
Tinder
Twitter/X
Unknown (Accommodation/Vacation Platforms)
Unknown (Auction/Purchase and Listing Platforms)
Unknown (Dating Platforms)
Unknown (Search Services)
Unknown (Social Media, Messaging and Call Platforms)
WhatsApp
Yahoo

What we are doing to drive better performance and improve outcomes for consumers in the payments industry?

We have adopted a multi-pronged approach to tackling APP scams across payment systems

The reimbursement requirement

In October 2024, we introduced a reimbursement requirement requiring payment firms to meet the cost of reimbursement. This incentivises industry to invest further in end-to-end scam prevention. It increases consumer protections so most victims of APP scams are swiftly reimbursed, boosting confidence in the UK payments ecosystem and reducing harm to payment users.

Improved scam prevention through data sharing

Innovative solutions to prevent scams are critical to strengthening the payments ecosystem. We want to support intelligence-sharing between payment firms so that they can improve scam prevention in real time – for example, stopping or delaying high-risk payments. From Q1 2025, we will work with industry and other regulators, such as the FCA, to better understand the best way to achieve system-wide protections to prevent APP scams.

Confirmation of Payee (CoP)

In 2019, we introduced the name and account-checking service, Confirmation of Payee (CoP), by directing the six largest banking groups to implement it. CoP has helped reduce some types of APP scams, as well as misdirected payments. In 2022, we expanded the requirement so that nearly all consumer payments would be covered. Since 2020 there have been 2.5 billion CoP checks conducted.

Protection of payment systems

We want Pay.UK, as the independent payment system operator, to run Faster Payments in a way that ensures customers are protected and scams are prevented from entering the system. We want Pay.UK to lead the development of protections for payment system users.

APP scams performance data

In 2023, we directed the 14 largest banking groups in Great Britain and Northern Ireland to provide us with APP scams performance data. For the last two years, we have published payment firm-level data showing the highest senders and receivers of APP scams, and how well these firms reimburse victims.

Data tables

Scams by sector

Rank	Category	Total Volume	% Share of Total	Total Value	% Share of Total
1	Social Media, Messaging and Call Platforms	124,057	56%	£67,429,184	20%
2	Auction/Purchase and Listing Platforms	29,473	13%	£21,283,030	6%
3	Telecommunications	26,975	12%	£107,229,381	31%
4	Entity Unknown	19,552	9%	£55,837,451	16%
5	Search Services	9,979	4%	£21,236,644	6%
6	Family/Friend	6,043	3%	£20,747,611	6%
7	Email	3,955	2%	£35,001,770	10%
8	Dating Platforms	1,414	1%	£10,098,612	3%
9	Accommodation/Vacation Platforms	1,086	Less than 1%	£1,719,409	Less than 1%
TOTAL		**222,534**	**100%**	**340,583,091**	**100%**

Data notes: The figures have been rounded up or down and may not equate to 100% across volume and value totals. The totals on this page also include aggregate data of all entities we collected data on.

Volume of APP scams in 2023 of the most common entities

Category	Sub-category	Invoice & Mandate Fraud	Impersonation Scam – Other	CEO Fraud	Impersonation Scam – Police/ Bank Staff	Investment Scam	Advance Fee Scam	Purchase Scam	Romance Scam
Email		1,301	842	153	169	253	500	–	–
Social media, messaging and call platforms									
	Facebook	26	1,403	10	40	1,402	4,035	67,337	719
	Instagram	2	681	4	7	2,418	1,277	11,885	511
	Snapchat	6	282	2	–	636	351	6,359	319
	Twitter/X	–	–	2	–	–	–	7,096	–
	WhatsApp	26	4,993	7	88	1,314	968	3,344	360
	Other	–	360	–	–	–	–	–	594
Accommodation/Vacation Platforms									
	Other	–	–	–	–	–	–	–	–
	SpareRoom	–	–	1	–	–	–	–	–
Entity Unknown		317	1,785	21	559	1,960	3,181	11,067	662
Auction/Purchase and Listing Platforms									
	Amazon	–	–	–	13	–	–	–	–
	Facebook	–	–	–	–	–	405	16,067	–
	Unknown	2	–	–	–	701	–	–	–
	Other	2	–	–	–	–	–	6,626	–
Telecommunications		235	9,529	13	8,990	1,694	3,234	3,088	192
Dating platforms									
	Unknown	–	–	–	–	–	–	62	370
	Other	–	–	–	–	–	–	–	526
Family/Friend		11	702	1	46	609	–	4,216	173
Search services									
	Google Search	10	–	–	7	–	1,675	–	–
	Unknown	26	348	–	49	664	1,442	–	–

Data notes: This table only contains data relating to the 10 highest entities who were most commonly reported as being used by fraudsters to carry out APP scams across each scam type. If an entity was not one of the highest 10, their data has been omitted.

Value of APP scams in 2023 of the most common entities

Category	Sub-category	Invoice & Mandate Fraud	Impersonation Scam – Other	CEO Fraud	Impersonation Scam – Police/ Bank Staff	Investment Scam	Advance Fee Scam	Purchase Scam	Romance Scam
Email		£22,639,756	£3,941,991	£2,297,287	£1,137,027	£3,683,699	£692,097	–	–
Social media, messaging and call platforms									
	Facebook	£11,916	£879,717	£2,365	£25,641	£5,044,028	£2,390,578	£19,509,964	£2,946,445
	Instagram	–	£282,821	£415	–	£2,855,774	£1,223,999	£3,292,556	£1,222,408
	Snapchat	–	–	£30	–	–	–	–	–
	Twitter/X	–	–	£70	–	–	–	–	–
	WhatsApp	£47,162	£8,238,709	£1,073	£484,000	£3,685,729	£1,591,288	£2,449,348	£903,261
	Other	–	£470,726	–	–	£1,781,063	–	–	£948,339
Accommodation/Vacation Platforms									
	SpareRoom	–	–	£750	–	–	–	–	–
Entity Unknown		£3,568,494	£5,326,016	£1,319,214	£3,975,928	£20,533,462	£7,852,261	£9,362,042	£3,900,035
Auction/Purchase and Listing Platforms									
	Amazon	–	£263,628	–	£167,868	–	–	–	–
	eBay	–	–	–	£86,400	–	–	£6,659,382	–
	Facebook	–	–	–	–	–	–	£5,444,785	–
	Other	£15,176	–	–	–	–	£434,725	£5,316,773	–
Telecommunications		£2,048,205	£20,941,262	£21,471	£57,719,548	£18,396,441	£5,904,924	£1,496,302	–
Dating platforms									
	Match.com	–	–	–	–	–	–	–	£1,097,171
	Plenty of Fish	–	–	–	–	–	–	–	£1,040,668
	Unknown	–	–	–	–	–	–	–	£2,911,538
	Other	–	–	–	–	–	–	–	£4,561,874
Family/Friend		£49,904	£1,200,068	£184,846	£274,914	£9,602,067	£1,828,793	£7,218,290	–
Search services									
	Google Search	£22,036	–	–	£27,558	£4,412,750	£717,019	£2,805,226	–
	Unknown	£12,504	£462,890	–	£301,022	£7,115,594	£883,930	–	£749,562
	Other	£2,400	–	–	–	–	–	–	–

Data notes: This table only contains data relating to the 10 highest entities who were most commonly reported as being used by fraudsters to carry out APP scams across each scam type. If an entity was not one of the highest 10, their data has been omitted.

Glossary

Concept	Definition
BACS Payment	Bankers' Automated Clearing Services. A Bacs payment is one of the most common bank-to-bank transfers in the UK. There are two main types of Bacs payment: direct debit, where one party has been given permission to pull money from the bank account of another party, and direct credit, where a party deposits the money in the other party's account.
BACS Standing Order	Pays a specified amount of money on a set date, similar to a direct debit. However, where a direct debit is giving permission to an organisation to take money from your bank account, a standing order is set up by the consumer with their bank.
CHAPS	Clearing House Automated Payment System. CHAPS is a sterling same-day system used to settle high-value wholesale payments as well as time-critical, lower-value payments like buying or paying a deposit on a property.
Consumer	A service user of a payment firm. These are individuals, microenterprises (enterprises that employ fewer than ten persons and have either an annual turnover or an annual balance sheet total that does not exceed €2 million) or charities (a body whose annual income is less than £1 million per year and is a charity as defined by the Charities Act 2011, Charities and Trustees Investment (Scotland) Act 2005 or the Charities Act (Northern Ireland) 2008).
Faster Payment	A payment made across the Faster Payments system.
Faster Payments	The UK electronic payment system that provides near real-time payments as well as standing orders and forward-dated payments, operated by Pay.UK. The service facilitates real-time payments of up to £1m – initiated primarily online, mobile, or via telephone banking. Over 90% of APP scam losses occur over Faster Payments, based on UK Finance data.
Financial Services (Banking Reform) Act (FSBRA) 2013	Legislation passed by the UK parliament that established the Payment Systems Regulator to ensure that payment systems are operated and developed in a way that considers and promotes the interests of all the businesses and consumers that use them.
International SWIFT	Payment messaging system standardising international monetary transfers between banks.
Intra Bank Transfers	Payments made from an account with a payment service provider to another account held with the same payment service provider.
Ofcom	The regulator and competition authority for communications services in the UK including online safety and telecommunications.

Glossary continued

Concept	Definition
Payment Service Provider (PSP)	A provider of payment services to customers typically through the provision of accounts. A PSP may be a bank, an e-money institution, a building society, or a payment institution. In the UK, a PSP must be authorised and regulated by the FCA. PSPs may be direct PSPs or indirect PSPs, depending on whether they are able to initiate payments directly in a payment system or only via an indirect access provider.
Payment system	A system made up of a series of steps that allow funds to be transferred between accounts, allowing people and businesses to move payments between one another.
Push payment	A monetary transaction that is sent ('pushed') by the payer to the payee, such as making a bank transfer to a friend or family member or passing cash to a cashier at a shop.
Reimbursement requirement	From 7 October 2024, PSPs must fully reimburse customers who have lost funds in an APP scam if they meet certain requirements. The cost of the reimbursement will be split 50/50 between the sending and receiving PSPs of the payment.
Section 81	Section 81 of the Financial Services (Banking Reform) Act (FSBRA) 2013, which gives the PSR powers to require any person (who may or may not be a regulated party) to provide information and documents which they require in connection with their statutory functions.
Specific Direction 18	A requirement from the PSR for the 14 largest GB banking groups in the United Kingdom to provide information about APP scam payments that they have sent. The PSR compiled comparisons of information for each directed PSP and certain receiving PSPs, and published these comparisons or extracts of these comparisons and will continue to do so periodically.
UK Finance	A trade association that represents more than 300 firms in the banking and finance industry in the UK.

© The Payment Systems Regulator Limited 2024

The Payment Systems Regulator Limited
12 Endeavour Square
London, E20 1JN

Telephone: 0300 456 3677
Website: www.psr.org.uk