

APPENDIX

Examples of scams, how they are carried out and statistical evidence.

Contents

Introduction.....	2
Romance Scams	2
Purchase Scams	4
Money Muling	11
Investment Scams	13
Scams via chat channels	14
Bank impersonation	14

Introduction

For the benefit of Ofcom, we have included examples below of some of the different types of fraud that commonly take place on online platforms. The below case studies are based on real-life reports that we have received from UK Finance member firms. Unless otherwise referenced, figures in this section are from UK Finance's Report: 2023 Half Yearly Fraud Update.¹

Romance Scams

What is a romance scam?

In a romance scam, the victim is persuaded to make a payment to a person they have met, often online through social media, dating websites and apps or gaming sites, and with whom they believe they are in a relationship.

The nature of the scam means that the individual is often convinced to make multiple, generally smaller, payments to the criminal, as indicated by an average of around five payments per case.

Whilst these frauds typically start on dating sites and apps or social media sites, the majority of cases move to instant messaging services such as WhatsApp.

What do romance scams cost to the economy?

A total of £21.2 million was lost to romance scams in 2020 (an increase of 17 per cent from 2019), affecting nearly 9,000 reported victims (32 per cent higher than 2019) - driven by the rise in online dating during the pandemic. Due to the emotional cost of such scams to each victim, it is difficult to only speak of such a scam in monetary values.

It also should be considered, this form of scam in particular relies on multiple payments hence a victim coming forward takes time leading to period under-reporting. More than economic cost, it is the emotional cost to each of the victims that also needs to be considered.

Romance scam case study

In October 2020, a 60-year-old male from London was searching for a companion using Google. He was directed to a third-party website promoted on Google where he was asked to subscribe to their service and then began interacting with a user purporting to be a 40 year-old female from Romania. *The fact that profile was fake and was operated by fraudsters who had cloned a genuine account from the platform so that it appeared legitimate was unbeknown to him at the time.*

Over the proceeding several months, messages were exchanged which led to a proposed meeting in London. The fraudsters convinced the user to transfer £2,000 for flights for the meeting. Shortly before flights were scheduled to take off, the fraudsters fabricated reasons why the flight had been missed and requested funds to pay for urgent medical care or customs duties.

This happened repeatedly and in total, £75,000 was sent to the fraudsters account.

What exactly is romance fraud, and how do criminals take advantage of the criminal activity?²

¹ <https://www.ukfinance.org.uk/system/files/2023-10/Half%20year%20fraud%20update%202023.pdf>

² <https://www.college.police.uk/article/romance-fraud-five-things-you-need-know>

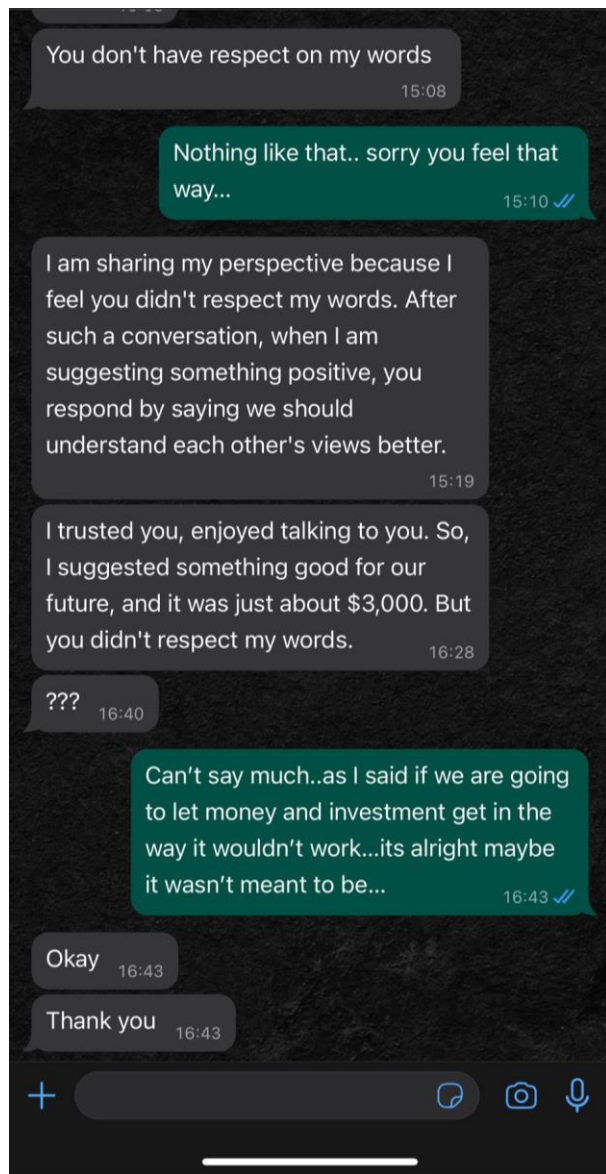
1. Romance fraud is one of eight high-priority crime types assessed by the City of London Police's National Fraud Intelligence Bureau (NFIB) as having a significant impact on UK citizens. Reports to Action Fraud have increased by 26% in the last year, with victims losing £10,000 on average.
2. Criminals use fake online profiles to form relationships with victims and make them think they've met their perfect partner, in order to get their money or personal information. This occurs on dating sites and other platforms that have a messaging function, such as Facebook, Instagram, and gaming sites and apps.
3. Red flags include the person making excuses why they can't meet or video chat, and the person claiming to be working overseas in a respectable profession, such as the military or an international charity. Romance fraudsters will talk to the victim for weeks, or even months, to build up their trust before creating a time-critical emergency that requires the victim's help. This is usually something emotive that pulls at their heartstrings, for example, paying an urgent medical bill for a sick family member.
4. A lot of romance fraudsters are based abroad, and investigations into suspects can be difficult. As the national policing lead for fraud, the City of London Police has set up a number of ways for police forces to disrupt romance fraud activity. Forces are able to alert money transfer services to suspect customer accounts. Forces can also now send intelligence referrals to the Ghanaian authorities where they have identified suspects who are based in Ghana.
5. Romance fraudsters don't just ask for money. They can also ask for:
 - access to the victim's bank accounts
 - loans to be taken out, or investments made, on their behalf
 - copies of the victim's personal documents, like a passport or driving licence
 - gift card codes
 - the victim to receive and/or send parcels

Romance scam leading to an investment scam

A consumer on a dating website looking for a connection is befriended, and an online relationship is formed. Over time rather than the victim being asked to pay money for fictitious legal or medical bills they are encouraged to make investments, opening e wallets with crypto exchanges, of which they give the fraudster access. The victim is then continually encouraged to pay in until such a time as they recognise they are being scammed or until someone intervenes to stop further payments.

Romance scam leading to an investment scam

In a recent example, a 36 year old man was contacted via a dating app by a 33 year old women. The women moved them onto a messaging service and over the course of a few weeks cultivated a relationship with him. It culminated with a request of £3000 in investment. Prudency prevented the scam from occurring in this case but the emotional damage of a relationship turning into a scam is still a valid consideration.



Romance scam leading to money mule

Very similar to the above, however instead of the victim being asked for money, they are asked to receive money and send it on to other accounts controlled by the fraudster. These funds would have originated from another fraud and this victim, in allowing their account to be used for the transfer of funds, is themselves involved in the facilitation of the crime.

Romance scam to sextortion (including the use of AI to create fake images)

These cases start as online relationships, with the fraudster making requests for payment. However, the relationship evolves when the victim is blackmailed by their 'partner', usually under the proviso that they have images (legitimate or AI-generated) that they will send to friends or family members unless a payment is made.

Purchase Scams

What is a purchase scam?

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 social media marketplaces, where scams are often promoted via paid-for adverts.

³ An extract of the messages exchanged.

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 cheap holidays, travel deals 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.

What do purchase scams cost the economy?

UK Finance half year fraud stats showed that 77,000 cases of purchase scams were recorded by UK banks in the first six months of 2023 alone – this is over 400 a day.

Top 10 scammed items on marketplaces

A UK Finance member has revealed that the most scammed items, which include household items, services, and personal purchases.⁴ In order by volume, these are:

	% of cases	Average loss
Vehicle/Parts/Hire	20%	£955
Concert/Event/Sports Tickets	11%	£193
Shoes/Trainers	8%	£174
Appliances/Gadgets	6%	£225
Clothing/Accessories	6%	£203
Tradesperson/Tools/Materials	6%	£1,358
Mobile Phone	5%	£275
Games Console/Games/Toys	5%	£144
Property/Rental/Accommodation	4%	£862
Furniture/Homeware	4%	£286

⁴ <https://www.tsb.co.uk/news-releases/tsb-issues-urgent-consumer-warning-over-purchase-scams-ahead-of-busy-online-shopping-period/>

Purchase scams case study- Online advertising of goods

An individual bought a laptop advertised on social media at a heavily discounted price compared to the one he had seen on the official seller's website.

Upon contacting the seller, the victim was told that the offer was for a limited time only therefore if they wanted the laptop, he needed to pay quickly by bank transfer.

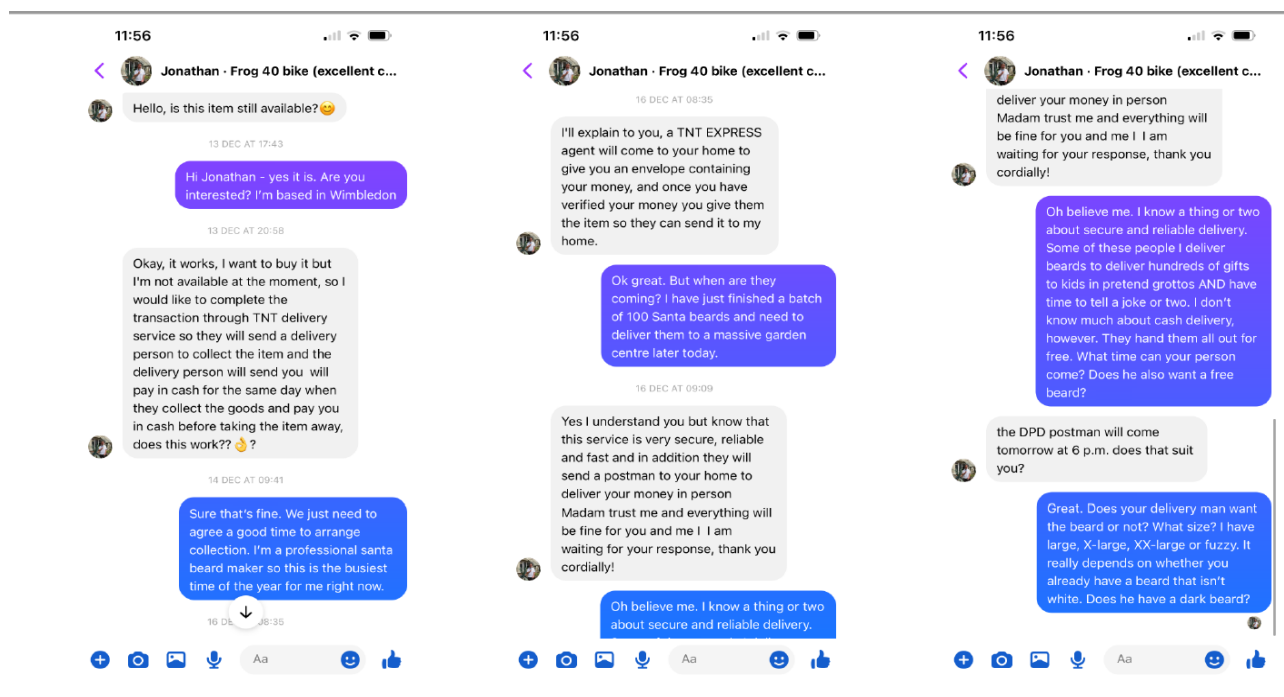
Proof of payment was sent to the seller but when the victim asked for a tracking number, he received no response. After numerous attempts to contact the seller, the victim searched their name and came across numerous bad reviews from other people. He never received the laptop.

Purchase Scam case study - Holiday booking site

A Family booked a holiday on a widely used aggregator website. The website's terms said that you could pay through the site, or alternatively they might be contacted by the letter with different payment terms. The website made it clear that they would not be liable for any payment that a customer attempted to make which was not on their platform but it allowed hyperlinks to other webpages on their site. The family member received an email with request to pay and it was a scam email. It turned out the property didn't exist, however even in such a case the platform refused to reimburse her. She was ultimately refunded by her bank!

Purchase scams morphing into courier scams case study

A member representative had an item for sale on a marketplace. The scamster contacted the representative to purchase the item and proceeded to suggest a courier service would come to pick the item and pay for the same. Even when reported to the platform (the representative reporting the event as a common citizen) the potential scamster was not removed from the website as it did not objectively go against their community standards.



Triangulation fraud case study

Triangulation fraud occurs when a customer makes a genuine purchase on a third-party marketplace, like eBay or Amazon, but the seller fraudulently purchases the product from another merchant. The name comes from the tri-lateral relationship between three involved parties: the unsuspecting customer, the legitimate merchant, and the fraudster middleman.

When these attacks are targeted they can put genuine and successful businesses in to compliance programs with the cards schemes and potentially drive them out of business.

Ghost Brokering - Case Studies (One Acquirer)

<https://www.thisismoney.co.uk/money/beatthescammers/article-10368215/The-online-schools-scammers-avoid-victims.html>



Retail Merchant - A retail merchant saw their fraud increase slowly from May - Sept where fraudsters were testing the fraud parameters set by the merchant. In October, the fraud increased sharply peaking at over £900,000 of reported fraud in November. The merchant adapted their fraud rules and the fraud stopped almost overnight reducing to a pre-attack level. **The total fraud reported for this attack was in excess of £1.6million.**



University - Foreign students were duped into paying their tuition fees to a ghost broker who offered a "special deal" on the fees if they went through them. This scam proved highly lucrative for the ghost broker who was paying the student's tuition fees using stolen credit card details and taking cash payments from the students. **The university saw over £400,000 of fraud reported against them from this attack.** There were very difficult conversations with their students who had unknowingly had their tuition paid for with a stolen credit card.

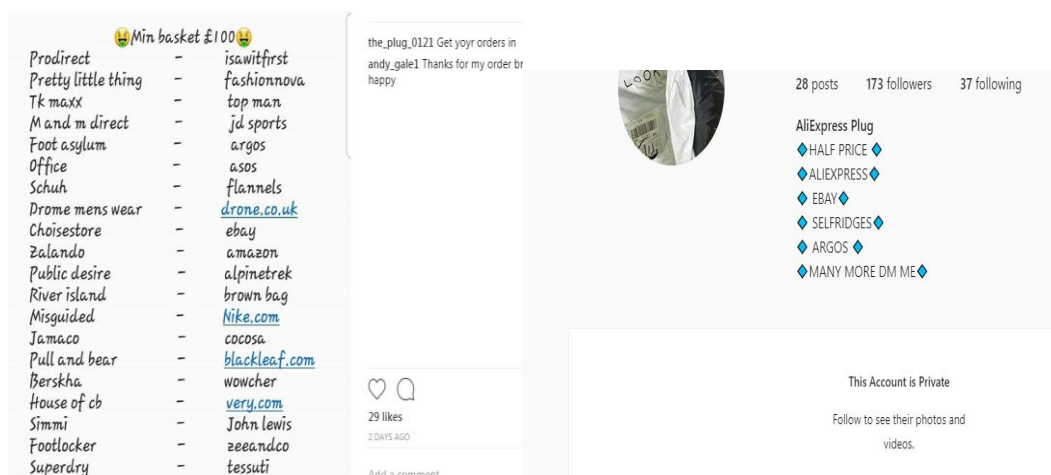


Fast Food Merchant - A fast food merchant was targeted by a highly organised group of ghost brokers who were offering half price food to members of the public, targeted the student population. Once the scam was understood and investigated, the merchant could see the fraudsters were working across several social media accounts and working in shifts to offer members of the public the same opening hours as the merchant they were targeting. **This merchant saw over £1million of fraud reported against them.**



Travel Merchant - A travel merchant suffered a ghost brokering attack where the fraudsters had opened a website and social media accounts to mimic the merchant's own online presence, and were able to drive traffic to them instead. The fraudsters were taking details from members of the public and direct payments, then making the booking on the travel merchant's site using stolen credit cards. **The total fraud reported exceeded £20million over a space of several months.**

Some examples of how these would appear in a user generated post.



Min basket £100 🙄

- Prodirect - isawitfirst
- Pretty little thing - fashionnova
- Tk maxx - top man
- M and m direct - jd sports
- Foot asylum - argos
- Office - asos
- Schuh - flannels
- Drome mens wear - drome.co.uk
- Choisestore - ebay
- Zalando - amazon
- Public desire - alpinetrek
- River island - brown bag
- Misguided - Nike.com
- Jama.co - cocosa
- Pull and bear - blackleaf.com
- Berskha - wowcher
- House of cb - very.com
- Simmi - John Lewis
- Footlocker - zeeandco
- Superdry - tessuti

the_plug_0121 Get your orders in
andy_gale1 Thanks for my order br happy

28 posts 173 followers 37 following

AliExpress Plug

- ◆ HALF PRICE ◆
- ◆ ALIEXPRESS ◆
- ◆ EBAY ◆
- ◆ SELFRIDGES ◆
- ◆ ARGOS ◆
- ◆ MANY MORE DM ME ◆

This Account is Private

Follow to see their photos and videos.

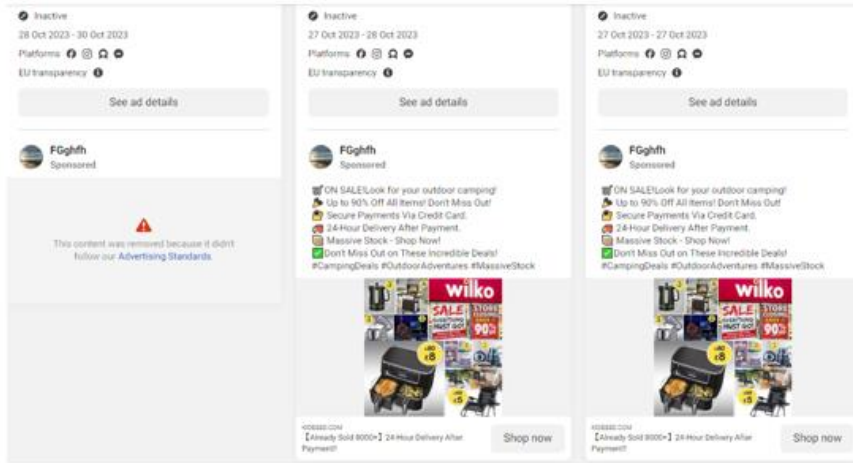
29 likes
2 DAYS AGO

Add a comment...

URLs in adverts

In a five-week period, post Wilko entering into administration, just one UK Finance member had more than 3000 victims and £600k attempted fraud as a result of these adverts appearing on a platform. Across the industry this would be 20k victims and £3.5mn of attempted fraud. Such scams rely on various forms of market disruptions or promises of heavy discounts to lure victims.

It may be noted that below examples of paid advertisements used in a Wilko Fraud Incident in Q4 2023 lured victims by offering heavy discounts during a cost of living crisis. Each advertisement was found to be up for between 1 and 2 days with a cumulative reach of 51,068.



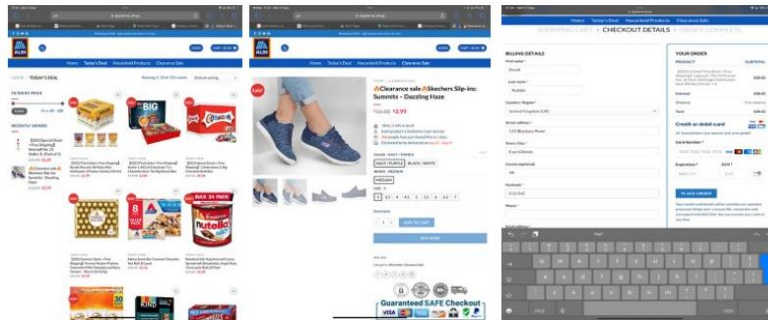
**Reach 49,587
(in EU)**

**Reach 825
(in EU)**

**Reach 656 (in
EU)**

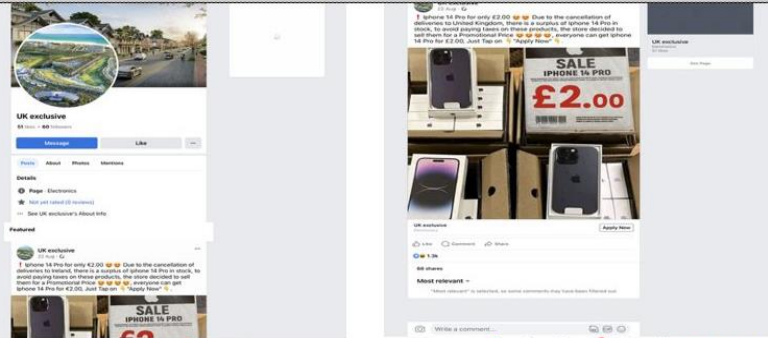
Example 2 – ALDI - <https://signerne.shop/>

- Customer spotted Facebook ad for an ALDI sale.
- Advert leads to the below website.
- Customer identifies items they wish to procure and proceeds to the payment screen disclosing necessary information for Apple / Google Pay enrolment.
- Customer receives Apple/ Google Pay activation OTP and discloses into website under the impression it is a 3DS step up.
- No transaction to ALDI is seen.
- Fraudulent token spend undertaken at Zettle.
- Customer reports fraud on their Bank account.

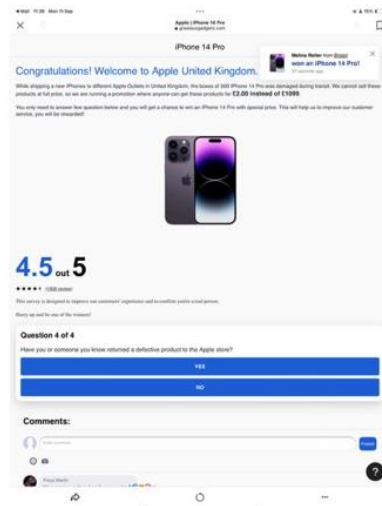
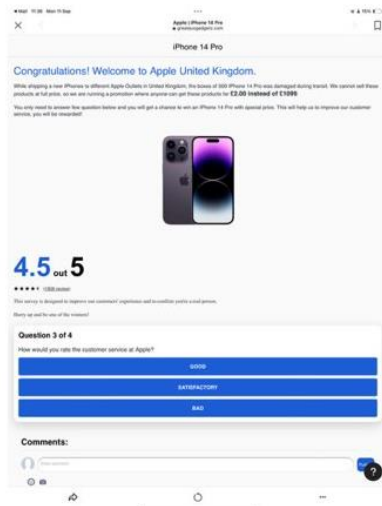
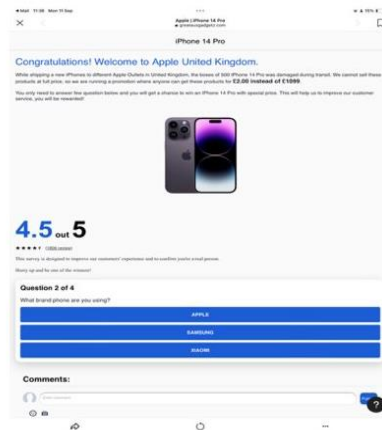
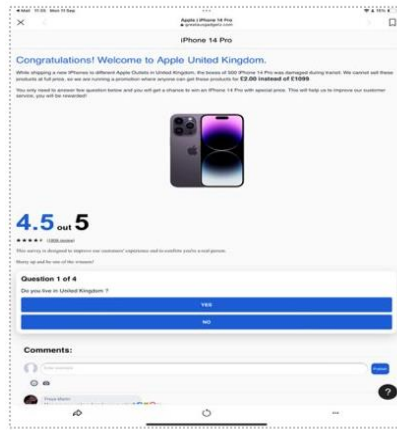


Example 3 – iPhone Scam - specialgiftszone.com

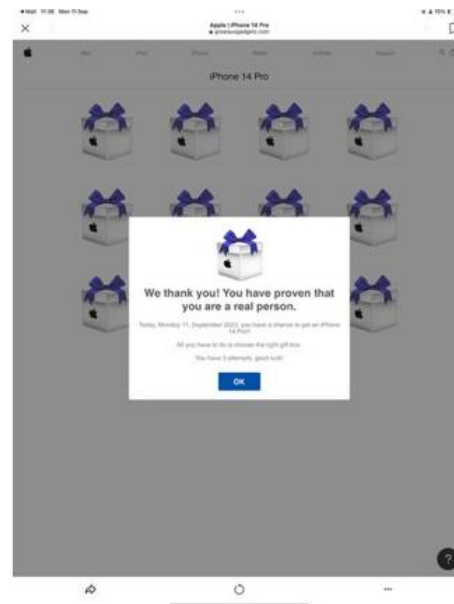
- Customer identified a Facebook advert offering an iPhone 14 Pro (c.c.1k RRP) for £2.
- Link within page took the customer to a webpage that asked a series of questions.
- Customer was advised that they were able to procure an iPhone for £2, if they found an iPhone behind a box within 3 guesses.
- Customer found an iPhone within the 3 guesses and as a result, was taken to a payment page.
- Customer disclosed personal & card information to be in receipt of their iPhone.
- Fraudster undertook a fraudulent Apple / Google Pay enrolment with the information the customer disclosed.
- Customer receives Apple/ Google Pay activation OTP and discloses into website under the impression it is a 3DS step up.
- Fraudulent token spend undertaken with transactions to Zettle seen.
- iPhone never arrives.
- Customer reports token fraud to the Bank.



Continued next page...



Continued next page

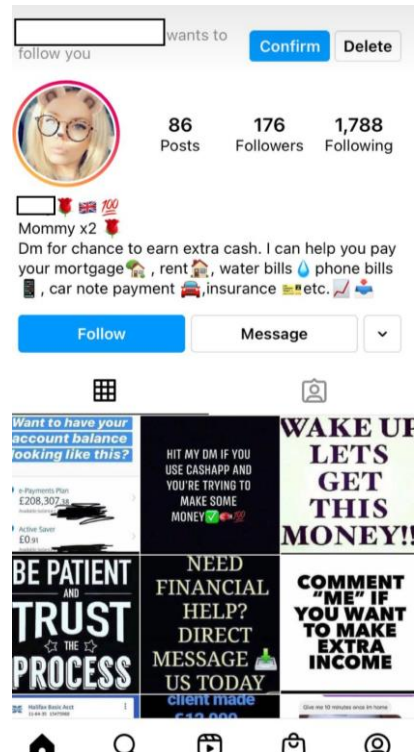


Emergence of criminals openly advertising fraud and scam services for sale online

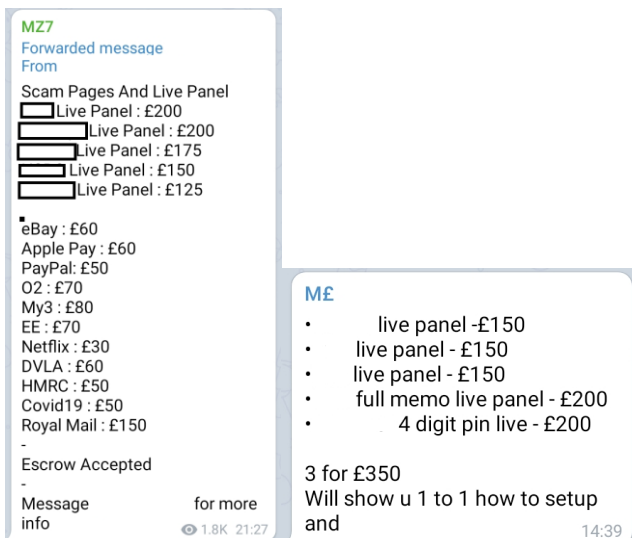
For the benefit of providing a holistic picture, we have included screenshots below illustrating how criminals openly advertise fraud and scam services for sale online, including template phishing websites and custom-built scam apps which replicate real banking apps.



Screenshot 1 – fraudsters have been targeting students into using fraud and scam services online, often through posts such as this screenshot from TikTok using the hashtag #scamtok. Whilst initially user-generated, these can also be promoted on users’ feeds by paid-for adverts to maximise the number of impressions. Note 121,000 likes on the post above.



Screenshot 2 – fraudsters also target individuals’ financial insecurities such as difficulties paying mortgage payments, rent and water bills. These can often lead to scams in themselves or move onto encrypted messaging services like WhatsApp or Telegram where criminals sell scam services (see screenshots below).



Screenshots 3 and 4 – fraudsters then move to encrypted messaging service platforms such as Whatsapp and Telegram to sell fraud and scam services online, including template phishing websites and custom-built scam apps which replicate real banking apps. Note 1,800 members in the Telegram group in Screenshot 3.

Money Muling

What is money muling?

Money mules are recruited, sometimes unwittingly, by criminals to transfer illegally obtained money between different bank accounts. Money mules, who are typically younger individuals (such as students), receive the stolen funds into their account. They are then asked to withdraw it and wire the proceeds to a different account, often overseas, keeping some of the money for themselves.

During the pandemic, money mule recruiters targeted 'generation Covid' – those looking for work or to earn easy money – by posting fake adverts on job websites and social media sites.

Often, people are unaware that allowing their bank accounts to be used in this way is a crime with consequences under criminal and civil law. Besides a criminal record, the individual could have their bank account closed and difficulty opening one elsewhere, and trouble obtaining mobile phone contracts or accessing credit in future.

What does money muling cost the economy?

Research from Cifas⁵ revealed there were 17,286 cases of suspected money muling activity. Younger adults, including all aged up to 30, now account for 64% of cases indicating money mule activity, and between January - June there were 11,015 cases filed that were indicative of money muling filed to the Cifas National Fraud Database.

Money muling case study

A 26-year-old male had a friend on Snapchat that he had known for a couple of years that asked for a favour.

A friend of the friend reached out to the male and asked him to receive money into his account, alongside receiving packages to his house which were then collected in person. Some of the packages contained iPhones, but the individual didn't know what was in all the packages. He was told that he would be paid for this but didn't keep any of the money that was moved through his account.

Money was transferred into other accounts of the customer as well as his account with the bank. The person he was in contact with had an active Snapchat account where he promoted stories of a lavish lifestyle which led the man to believe this activity to be legitimate. After failing to be paid, the male contacted the police, where he informed them and the bank of the activity he had taken part in. We do not know if any action was taken by the police to reprimand the individual, however the bank made the decision to close his account down.

Mule herders try to lure people into becoming mules complicitly or uncomplacitly ⁶

⁵ <https://www.cifas.org.uk/newsroom/cifas-ukfinance-lessonsplans-moneymules>

⁶ <https://www.moneymules.co.uk/tips/>

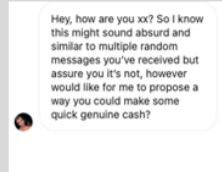
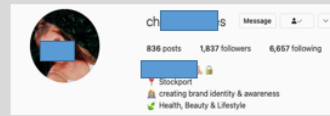
Mule Herder Archetypes – The Misleading

Offers money making opportunities, but is often vague about their nature

Makes use of video 'testimonials' from purported 'clients', but little to no elaboration on how money is made

Often use a fully developed persona – typically an attractive female. This may involve stealing images from a legitimate [user](#), or paying a skill.

Recruit unwitting mules



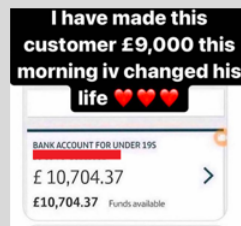
Mule Herder Archetypes – The Lifeline

Specifically target economically vulnerable groups.

Often predatory – assessed to crawl through social media seeking targets for recruitment.

Present themselves as a 'way out' for those in debt or otherwise struggling

Like the previous archetype, will often front their pages using models.



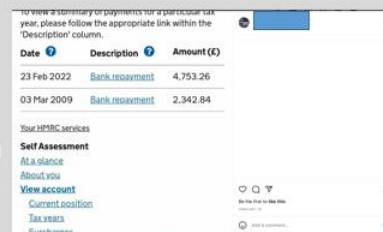
Mule Herder Archetypes – The Refund Specialist

Disposition varies – some may purport to offer a legitimate 'refund service', whereas others are more blatant.

These herders often target HMRC with fraudulent self-assessment claims, made using the mule's ID and UTR.

They may also fraudulently reclaim paid Direct Debits.

Tend to be most active near HMRC's annual self-assessment deadline.

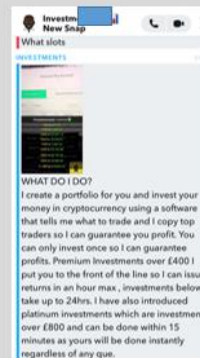


Mule Herder Archetypes – The Investor

Recruit money mules under the guise of an investment service.

These can be difficult to distinguish from outright investment scams...

...but some actors may be involved in both – IE a 'money flipping' scam which turns an 'investor' into a mule later.



The most brazen type of herder – they make little to no effort to hide the nature of their activity.

Will provide detailed instructions to mules, including which accounts to open, and how to respond to questions from the bank.

May claim to have insider connections

Spark 'herd mentality' amongst other mule herders.



Investment Scams

What is an investment scam?

In an investment scam, a criminal convinces their victim to move their money to a fictitious fund or to pay for a fake investment. These scams are often promoted through adverts on social media sites or search engines offering higher than average returns and may lead to cloned/fake websites impersonating real investment firms.

Criminals have been increasingly preying on people's financial insecurities during the pandemic through investment scams promising high returns. Some criminals may initially pay out returns on their victim's investment to convince them to invest more money.

How much does investment scams cost the economy?

Investment scam losses decreased by two per cent in January to June 2023 to £57.2 million. After the peak seen in 2021 during the pandemic losses and case volumes have levelled out, this is likely a combination of factors including fewer opportunities for criminal(s) 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 continued to account for the largest value of all eight Authorised Push Payment (APP) scam types with losses of £57.2 million or 24 per cent of the overall total.

Individuals of all ages are at risk from investment fraud as criminals target them by exploiting online services. Anecdotal intelligence suggests younger individuals may be more vulnerable to malicious social media posts promoted via paid-for adverts offering false investment opportunities, whilst older generations are more likely to fall victim to fake comparison sites or search engines which push victims to cloned investment sites. Indeed, National Fraud Intelligence Bureau statistics based on a rolling 13 months of data from Action Fraud⁷ shows that the number of investment fraud victims are broadly evenly split across the 20-79 age ranges.

Investment scam case study

A retired NHS employee in his 80s encountered an online advertisement for investments in Bitcoin. He was drawn to the advertisement because it included a purported endorsement from former Manchester United manager Sir Alex Ferguson, which gave him some comfort that this was a legitimate investment. *It must be stressed that the endorsement was fabricated and there was no connection with Sir Alex, however the victim did not know this at the time.*

The fraudsters were using a company name that was very similar to that of a genuine FCA-authorized investment company. Although there were some online reports indicating that this was a

⁷ <https://colpolice.maps.arcgis.com/apps/opsdashboard/index.html#/60499304565045b0bce05d2ca7e1e56c>

scam, the victim spoke to representatives of the company who were very articulate and convinced him that the negative reports were defamatory reviews from their rivals. He was promised substantial returns and began making deposits into a crypto-currency e-wallet set up in his name.

The funds were immediately paid away into the fraudsters' accounts. The victim lost £250,000, which was his life savings. His bank is supporting attempts to recover the funds.

Crypto Investment Scam

A UK Finance member customer interested in invested in cryptocurrency following review of influencers on social media platforms. This influencer had a large number of followers (over 100,000), showcasing wealth and lifestyle, posing with designer goods (cars, watches and luxury accommodation etc.).

Influencers advertised they accumulated their wealth via investment in crypto currency and encourages follower to private message them to "get rich quick". The customer contacts influencer initially via social media platform (Instagram) and the influencer moved communication quickly to a prominent messaging platform.

The customer started investing small amounts, then was requested further investment needed for return, following a further series of payments totalling £50k customer attempted to access their investment portal and influencer withdraws contact, blocking customer on all platforms.

The customer had no warnings/friction from social media platform around investments of this type or the risks of being request to communicate via another messaging platform. The customer has now contacted their bank to raise a claim.

Scams via chat channels

The growth of free messaging channels has created the potential for weaponizing and scaling scam attacks. Some messaging applications allow for creation of bots for various purposes allowing for greater targeting by criminals.

Messaging Scam Case study

A Customer received a message on WhatsApp saying 'Hi Mum, dropped phone in sink, it has water damage, this is my new number.' Customer was asked to make a payment for crypto, her daughter had never mentioned any interest in crypto before but the customer did not want to disappoint daughter so sent the payment.

The customer made one payment of £2,100 which was flagged by the Banks transaction monitoring systems, this included a confirmation of payee no match. The customer called her Bank to release the payment and the Bank warned her about WhatsApp impersonation scams, how they work and how to protect herself from such scams.

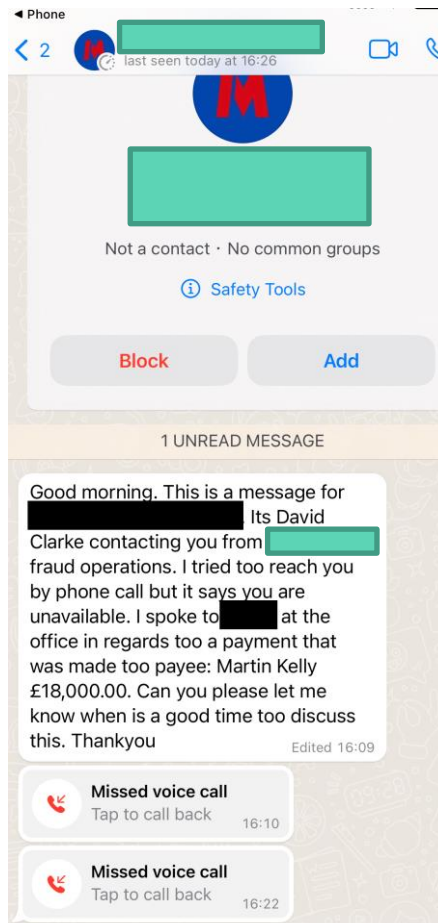
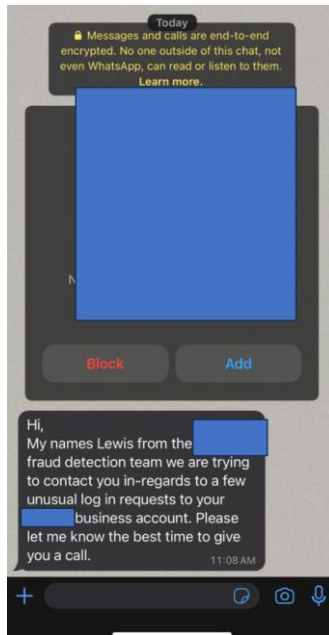
Further communication between the scammer and customer continues where they coached the customer to send the payment without any further checks. The next morning the customer received a message from her daughter`s genuine number and realised she had been scammed.

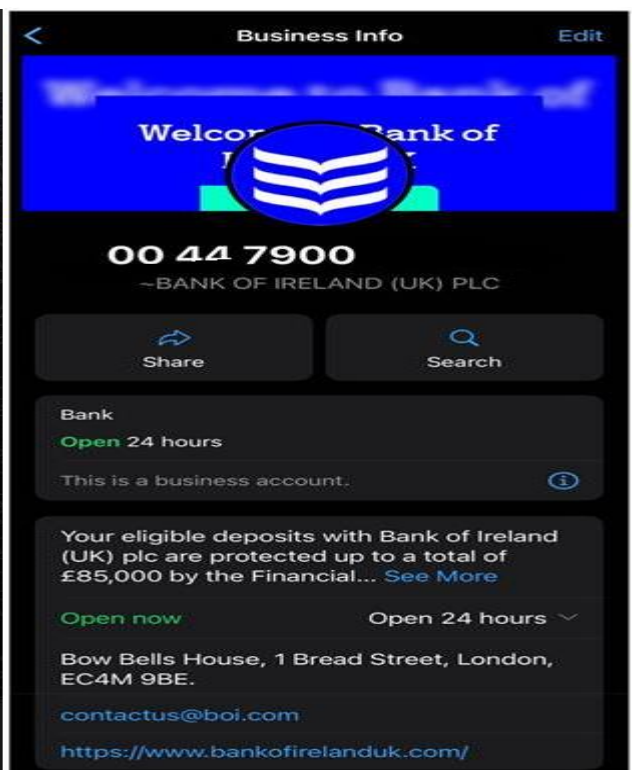
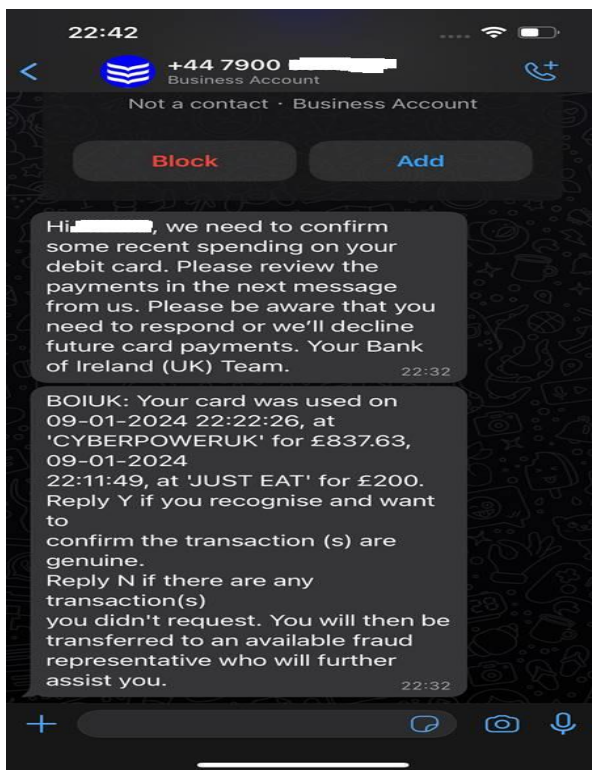
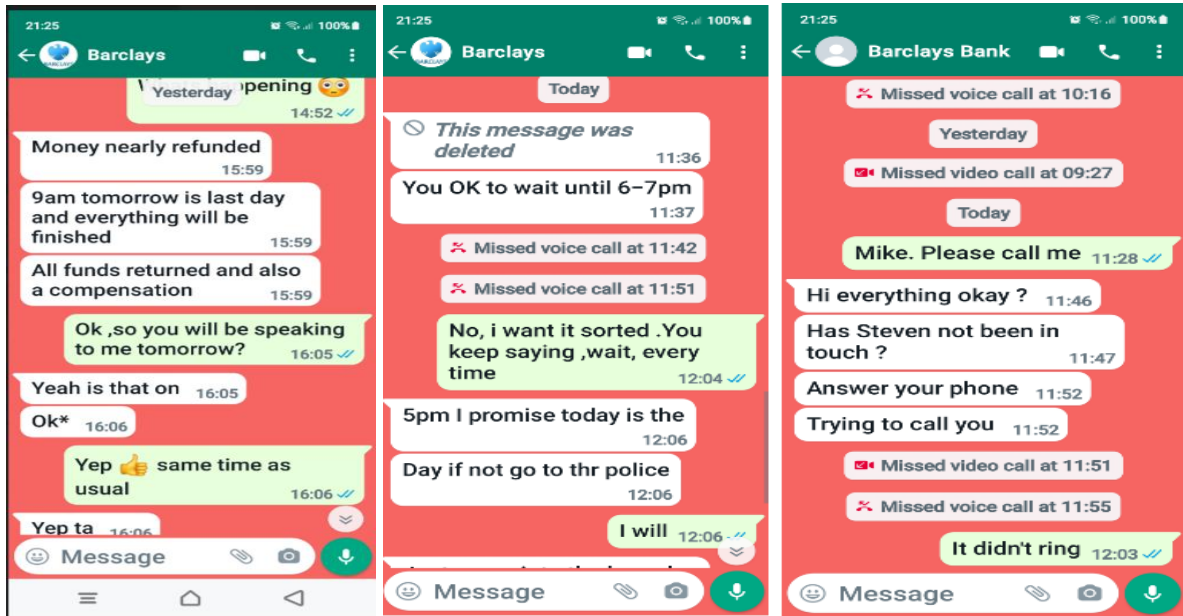
In this particular case the bank did attempt to add a level of friction for the customer but warnings and controls in social media platforms would support strengthening prevention.

Bank impersonation

This attack is not limited to any particular platform and it happens on multiple platforms where there are weak onboarding controls for trusted brands. To resolve this is a lengthy and slow process, often after victims have suffered harm.

Bank impersonation case study



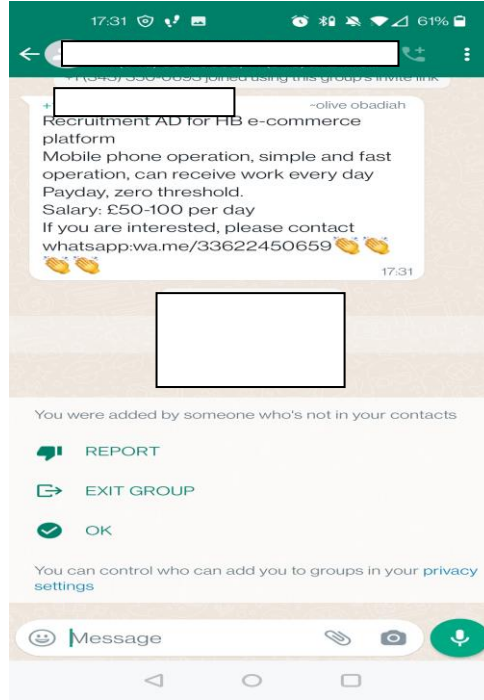
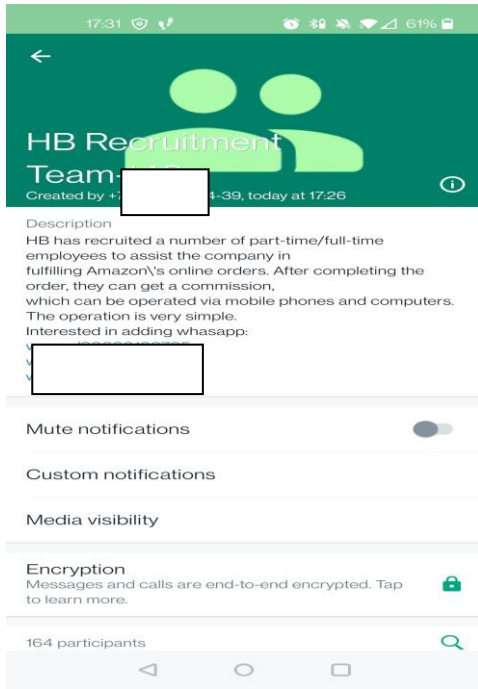


The profile was sending messages designed to look like card fraud alerts. The WhatsApp profile is shown below along with a screenshot of fraudulent messages received by a customer. The customer recognised the messages as fake so didn't reply.⁹

Group chat Job hire Screenshots

⁸ WhatsApp Business profile impersonating Bank of Ireland UK around 10th January 2024.

⁹ Bank of Ireland reported the profile to WhatsApp through the in-app reporting mechanism but didn't get any acknowledgement or reply from WhatsApp/Meta. The profile remained live until they reported the profile URL as fraudulent through their takedown provider – this can be done by reporting the URL in the format hXXps://wa[.]me/[phone number]



Mum and Dad Scams

In recent years, mum and dad scams have shown a significant uptick. These forms of scams are launched using messaging and social media platforms where a fraudster texts various individuals impersonating the child. The scamster proceeds to try to obtain money from the victim by suggesting the child has lost/broken their existing phone and they require funds to obtain a new device or have to pay bills

