



TWO-THIRDS OF ALL ONLINE SHOPPING SCAMS NOW START ON FACEBOOK AND INSTAGRAM

- **Social media platforms fuelling surge in online shopping scams**
- **Someone falls victim on Meta-owned platforms every seven minutes**
- **Estimated £27m being lost by UK consumers each year**
- **Lloyds Banking Group calls for technology companies to act**

Purchase scams starting on Facebook and Instagram are expected to cost UK consumers more than £27m¹ this year alone, according to new analysis by Lloyds Banking Group.

The rising popularity of online shopping has been accompanied by a surge in criminals tricking people into paying for goods and services that don't exist. Victims are lured in by the promise of cut-price or hard-to-find items, often advertised via social media.

They are asked to send money directly from their account to another account via bank transfer (also known as a Faster Payment), which provides very little consumer protection when something goes wrong.

New research by Lloyds Banking Group, based on analysis of reported cases among their more than 25 million retail customers, has found that two-thirds (68%) of all purchase scams now start on just two Meta-owned social media platforms – Facebook (including Facebook Marketplace) and Instagram. This accounts for around 40% the total amount lost to this type of scam.

Based on latest industry figures, that means someone in the UK falls victim to a shopping scam across these two platforms every seven minutes², costing consumers more than £27m a year.

The bank found that clothes, trainers, gaming consoles and mobile phones are among the most common goods being falsely advertised. Across the industry the average amount being lost by the victims of purchase scams is around £570.

Liz Ziegler, Fraud Prevention Director, Lloyds Banking Group, said:

“Social media has become the Wild West of online shopping in recent years, with very few checks in place to verify who is selling what. This has left consumers increasingly exposed to ruthless fraudsters, with hundreds of new victims targeted every day and tens of millions of pounds flowing to organised crime gangs each year.

“Banks have been at the forefront of tackling the epidemic of scams, but they cannot fight it alone. It's high time tech companies stepped up to share responsibility for protecting their own customers. This means stopping scams at source and contributing to refunds when their platforms are used to defraud innocent victims.”

Why banks can't fight fraud alone

It's right for the financial sector to play its part in fighting fraud, and banks have been at the forefront of efforts to stop scams and refund those who have fallen victim.

All major banks use sophisticated fraud detection systems, with every transaction being screened in real-time. If they spot something that looks suspicious, they can block the transaction, and the Government has helpfully committed in its recent National Fraud Strategy to allow banks more time to slow down suspicious payments.

But the reality is that almost 80% of scams start in the tech sector. By the time a victim reaches the point of making a payment through their bank account, it is very difficult to detect amongst the billions of genuine transactions which take place each year. Fraud is linked to only 0.01%³ of all Faster Payments (equivalent to one in every 10,000 transactions) made across the UK.

Take purchase scams as an example – as these make up the majority of all reported scams – where a customer is typically transferring just a few hundred pounds from within their own secure online banking account. There is often nothing unusual happening at the point the payment is being made to indicate to the bank that its customer is being scammed.

Lloyds Banking Group has invested hundreds of millions of pounds in advanced security systems to protect its customers, alongside employing thousands of staff dedicated to fighting fraud. It already reimburses the majority of scam victims.

However, reimbursement does not fully address the emotional trauma of becoming a victim of fraud, nor does it stop the flow of money to organised crime. Falling victim to a scam is profoundly distressing and casts a long shadow beyond the financial impact, including on mental health and confidence, leaving people deeply affected by the experience.

Relying on the banking sector alone to detect scams and provide refunds means those platforms where the vast majority of the fraud starts have no incentive to stop it.

Lloyds Banking Group is calling for technology and telecommunication companies to do more to stop scams at source and play their part in refunding victims of fraud which originates on their platforms.

Top tips to stay safe from online shopping scams

- **Be cautious on social media** – you don't know if the user profile and item are genuine, and have few ways of checking. A good rule is to only buy things you have seen in person.
- **Avoid deals that look too good to be true** – adverts with low prices or for sold-out items should ring alarm bells. Look for similar offers elsewhere to work out if they're realistic.
- **Buy from trusted retailers** – this is usually the safest way to shop online. But watch out for fake websites and emails, and be wary of mixed, bad or no reviews at all.
- **Use your debit or credit card** – this helps to protect your money should something go wrong. PayPal is another option that's usually safer than paying by bank transfer.
- **Pay attention to warnings** – your bank is likely to provide a warning when you set up a new payee or make an unusual payment. Be sure to follow any advice provided.

Notes to editors

About Lloyds Banking Group:

Lloyds Banking Group (LBG) is a leading financial services group and the UK's largest retail bank. Its brands, services and business span every aspect of banking and finance, including some of the biggest names on the high street, such as Lloyds Bank, Halifax and Bank of Scotland.

Methodology:

- 1) £27m figure based on proportion of losses (value) attributed to purchases scams originating on Facebook and Instagram (41% - LBG data), applied to total value of losses from purchase scams across the industry in 2022 (£67m - UK Finance data).
- 2) Seven-minute figure based on proportion of purchase scam cases (volume) originating on Facebook and Instagram (68% - LBG data) applied to total volume of purchase scam cases across the industry in 2022 (117,170 - UK Finance data) compared to total number of minutes in a year (i.e. 365 days x 24 hours x 60 minutes = 525,600 minutes).
- 3) 0.01% figure based on total volume of faster payments in 2022 (3.9 billion, Pay.UK data) divided by total volume of Authorised Push Payment (APP) transactions reported across the industry in 2022 (372,266 - UK Finance data).

Sources:

- **Lloyds Banking Group data source:** Figures based on analysis of relevant purchase scams reported by Lloyds Banking Group customers during January-December 2022.
- **UK Finance data source:** [Annual Fraud Report 2023_0.pdf \(ukfinance.org.uk\)](#)
- **Pay.UK data source:** [Faster Payment System statistics \(wearepay.uk\)](#)

Press office contacts:

Gregor Low / 07500 078 879 / gregor.low@lloydsbanking.com

Lynsey Cheshire Willis / 07595 124 924 / lynsey.cheshire-willis@lloydsbanking.com

"This report is prepared from information that we believe is collated with care; however, it is only intended to highlight issues and it is not intended to be comprehensive. We reserve the right to vary our methodology and to edit or discontinue/withdraw this, or any other report. Any use of this information for an individual's own or third-party purposes is done entirely at the risk of the person making such use and solely the responsibility of the person or persons making such reliance." © Lloyds Banking Group plc all rights reserved 2023.