LexisNexis®
RISK SOLUTIONS

Annual Cybercrime Report

UK Analysis

What is the Cybercrime Report?

The LexisNexis® Risk Solutions Global Cybercrime Report is based on cybercrime attacks detected by the LexisNexis® Digital Identity Network® from January-December 2022, during near real time analysis of consumer interactions across the online journey, from new account creations, logins, payments and other non-core transactions, such as password resets and transfers.

This UK subset analysis concerns UK-based transactions occurring in 2022. Attacks referenced in the report are based upon “high-risk” transactions as scored by customers.

Due to a large majority of UK ThreatMetrix™ customers being financial services organisations, the data should only be considered indicative and not representative of online transactions across all sectors.

The Global Annual Cybercrime Report, is also available now.

Overall UK transactions

Comparing UK and global transaction volumes.

UK Transactions:

15.8B

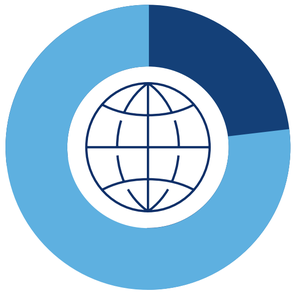
+29% Growth rate year on year

VS

Global Transactions:

78.0B

+24% Growth rate year on year



Around a fifth

of all global online transactions within the Digital Identity Network occur in the UK, which is the 21st largest country by population.

Expert view:

Total fraud losses (authorised and unauthorised) were down 8% year on year compared to 2021 according to UK Finance. Banks and card companies prevented £1.2 billion of unauthorised fraud – equivalent to 61p in every £1. Losses from card ID theft increased 97% per cent in 2022 compared with 2021, totalling £51.7 million, while third party application fraud is up 3%. Authorised push payment (APP) fraud – whilst still representing 40% of all fraud cases – saw a decrease in the value of losses in 2022. This reflects the mature nature of the UK financial services market with robust, hi-tech anti-fraud solutions in place by banks and fintechs, as well as high adoption of relatively more secure channels such as mobile and apps.

LexisNexis® RISK SOLUTIONS

Attack volumes by type:

Amongst the billions of UK transactions processed by the Digital Identity Network, the following attacks were recorded:

Human initiated

36M x**2** year on year

92% ▲ since 2021

This highlights the extent of the 'scam-demic' rampant in the UK.

VS

56% ▲ since 2021

Globally we saw a slower rate of growth.

Bot attacks

What is a bot attack? See in side bar

352M were identified in 2022

81% ▲ year on year

Bot attacks now represent around 2% of all online transactions processed by the Digital Identity Network in the UK.

VS

27% ▲ since previous year

Steep increase in attacks shows **UK is an important source** of bot attacks globally.

What is a bot attack?

Bot attacks are large-scale automated cyber attacks using sophisticated algorithms and automated scripts. Their objective can vary, from disrupting a particular website or organisation, to stealing data (such as in phishing and smishing attacks) to make fraudulent bulk purchases, or to perform other malicious actions. Attacks can be deployed against many different targets, such as websites, servers, APIs, and other endpoints. Recent waves of attacks have focussed on credential testing – i.e. bulk-testing stolen login details. Unfortunately, since many consumers still use the same username and password combinations for multiple online accounts, this process can help criminals to both gather data for scams or even access victims' banking services.

LexisNexis® RISK SOLUTIONS

Overall attack rate

The overall attack rate is the number of confirmed human initiated fraud attacks, as a proportion of overall transaction rates.

UK: **0.2%**

Global average: **1.3%**

- The UK enjoys lower overall attack rates than the rest of the world.
- This is in large part due to UK institutions adopting sophisticated tech-based fraud prevention solutions, which helps catch much of the traditional, large scale 3rd party fraud that remains an issue in most other parts of the world.
- Inevitably, new fraud types are emerging to fill this vacuum, including First Party Fraud – now a significant problem in the UK – and Synthetic Identity Fraud, a lesser, but growing issue.
- A lower attack rate can also be attributed to volumes of 'trusted' customer traffic accessing UK digital banking services, particularly via mobile app.
- See more on trusted transactions and mobile volumes on the next page.

Why does the UK market enjoy higher levels of trust?

The UK is among the most mature global markets in the development and adoption of fraud prevention tools.

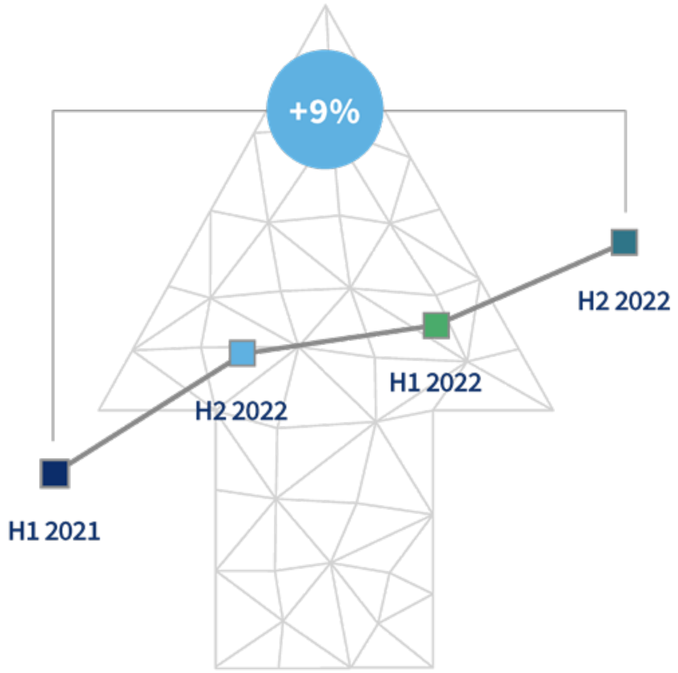
This enables financial institutions using AI and machine learning to combine fraud data and trends, behavioural risk signals and device and geo-location information from which complex and organised fraud attacks can originate. This intelligence is the shared on a privacy by design principle with other organisations in the banking and other sectors.

Such global enterprise solutions provide a platform for real-time collaboration, answering the industry's call for a greater access to shared data to make intelligence-led decisions. Analysis of dynamic user behaviour helps build more accurate risk models, resulting in fewer false positives and the lowest possible fraud levels.

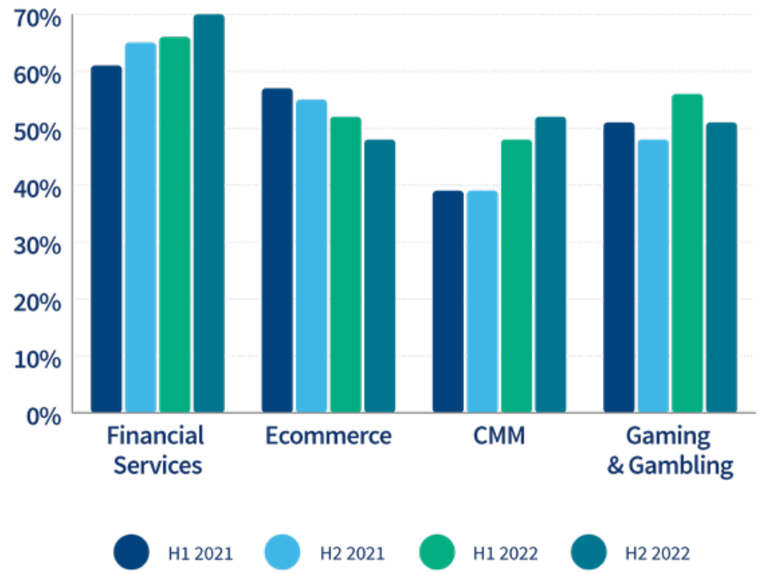
LexisNexis® RISK SOLUTIONS

Trusted traffic

% of global transactions marked as trusted



% trust per industry



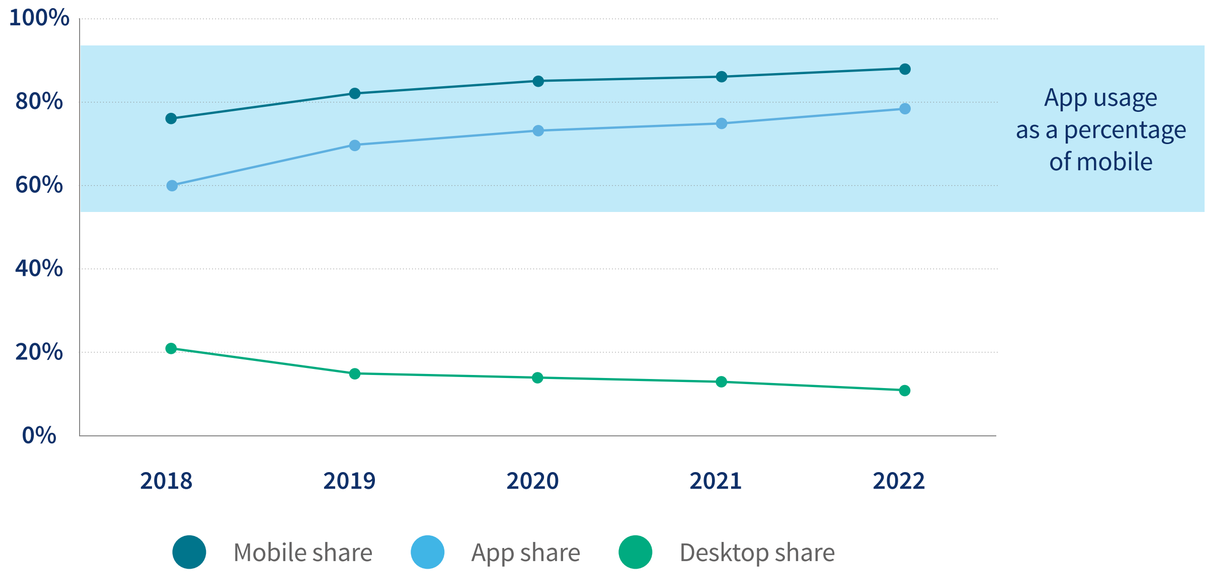
Global volumes of trusted traffic, by sector.

- As fraud attacks increased during the past 18 months, organisations have responded by focusing more on building trust with their loyal customer base.
- A significant volume of trusted customer traffic is accessing UK digital banking services.
- This is helped by the large adoption of mobile and app-based online banking services, leading to significant volumes of traffic processed in those channels [see page 7 for more].
- This is also playing a part in keeping the overall fraud attack rate low.
- As well as preventing fraud, the increase in volumes of trusted customers means a better experience for those genuine, returning customers.

LexisNexis® RISK SOLUTIONS

Mobile’s rise to dominance

Mobile and app versus desktop usage



The Digital Identity Network differentiates between transactions carried out on desktop and mobile, and between mobile transactions carried out via an app, or the device’s internet browser.

- In the financial service sector in particular, the mobile channel continues to dominate with almost 9 in 10 (88%) of UK transactions processed on the mobile channel.
- Apps dominate within the mobile channel, representing 89% of transactions processed in 2022.
- Growth in the mobile channel has been steady over the past five years – looking at transactions processed in the digital identity network.
- The global average of transactions processed for the mobile channel is 77%.

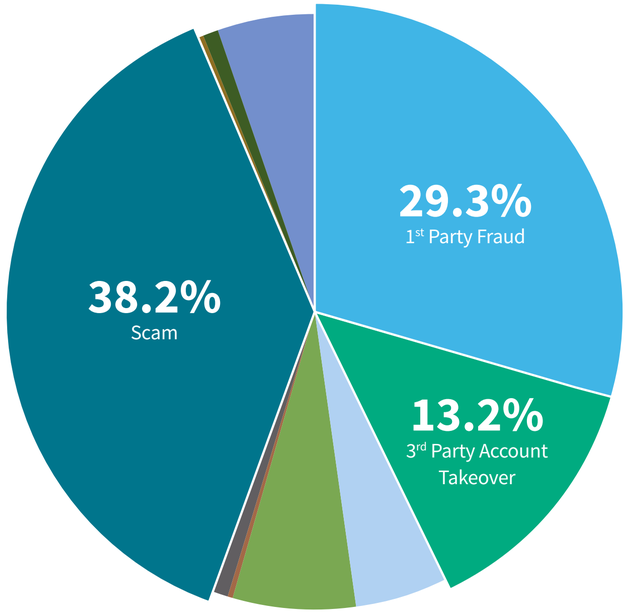
Fraud view:

Although loss values are low compared to other fraud types, mobile banking fraud is on the rise with a third (33%) increase in losses in 2022 and a 10% increase in volumes, compared to the prior year, according to UK finance. This increase in fraud corresponds to the rise in banking apps which are now used by over half (53%) of UK adults. This reflects banks’ mobile-first approach to online banking services, offering a low friction experience with device identification and biometrics.

LexisNexis® RISK SOLUTIONS

UK Fraud split

Fraud Classification (UK)



- 1st Party Fraud
- Scam
- 3rd Party Account Takeover
- True Identity Theft
- Synthetic Identity Theft
- Bonus Abuse
- 3rd Party Chargeback Fraud
- 1st Party Chargeback Fraud
- 2nd Party Fraud Collusion
- Sim Swap Fraud
- Buyer Fraud
- Malware
- Other

There are three dominant forms of confirmed fraud being reported by customers of the Digital Identity Network in the UK, which are predominantly financial services organisations.

- Scams: including social engineering and APP scams, such as romance and investment scams.

- First-party fraud: any fraud committed against a financial institution or merchant by one of its own customers. This can include individuals or groups misreporting their identity and/or giving false information when applying for services, such as credit cards, with no intention to repay.

- Third-Party account takeover fraud accounts for nearly 1 in 7 confirmed cases: the lower volumes of this fraud in the UK can be attributed to the wider adoption of modern tech-based prevention solutions which helps catch much of the traditional, large scale 3rd party fraud.

Fraud view:

These classifications are closely mirrored by UK Finance's figures for 2022 which show that scams represent around 40% of total losses and account takeover fraud representing around 13%.

LexisNexis® RISK SOLUTIONS

LexisNexis®
RISK SOLUTIONS

For more information, call **029 2067 8555**

or email **uk-irl-enquiry@lexisnexisrisk.com**

risk.lexisnexis.co.uk