Experian interactive report

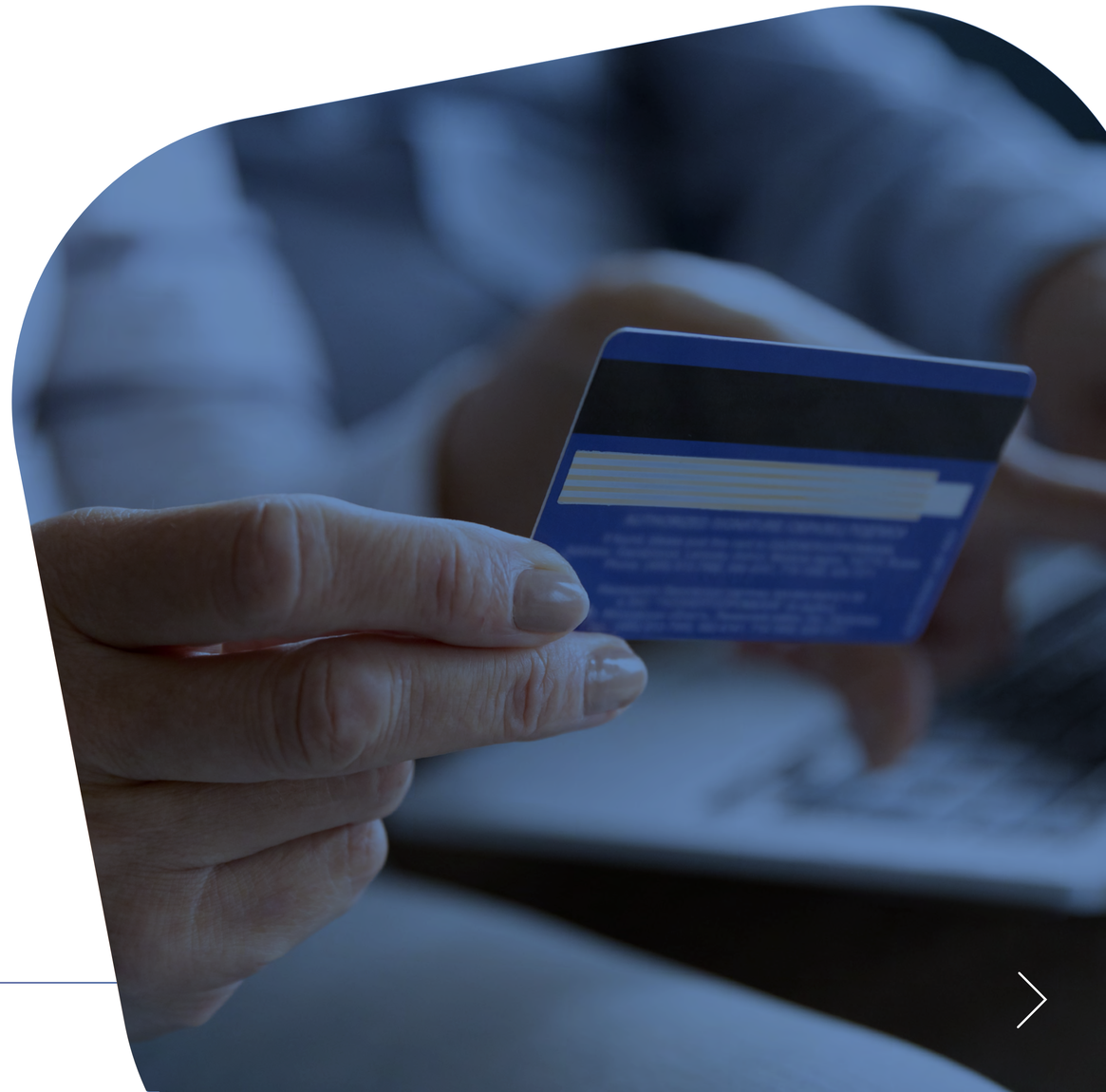
Six key UK fraud trends to watch out for in 2022

January 2022

"The rapid digitisation of the economy, turbo-charged by the Covid-19 pandemic, has presented new opportunities for all types of business. But the acceleration also brings challenges; businesses are under more pressure than ever before to offer secure, seamless, and efficient customer journeys to run a successful digital operation.

Consumers' growing digital-first approach, also brings risk. Fraudsters are finding new and innovative ways to commit fraud and steal people's identity, personal details and money."

Eduardo Castro,
Managing Director, Identity and Fraud, Experian UK&I



Here are six trends we expect to see develop in the UK over 2022:

- Cryptocurrency scams
- Ransomware attacks
- Text and cold-calling scams
- Digital payments fraud
- Social media oversharing
- Changing fraud profiles

Cryptocurrency scams

The advertising of cryptocurrencies, particularly on social media, has become commonplace but it's a fertile ground for scammers.

According to Action Fraud more than

£145 million

was lost to crypto fraud scams by British consumers in 2021, with younger people (18-25) the most targeted.

The majority of firms selling cryptocurrencies as an investment are unregulated, so there's no recourse for the consumer if they become a victim. We expect this trend only to become more severe over the next 12 months.

Cryptocurrency scams | Ransomware attacks | Text and cold-calling scams | Digital payments fraud | Social media oversharing | Changing fraud profiles

Ransomware attacks

A new avenue of attack for fraudsters is through ransomware. The National Cyber Security Centre (NCSC) dealt with a record number of incidents in 2021, in which criminals prevent companies and other organisations from accessing their data unless a ransom is paid.

Across the globe, **ransomware attacks will be a significant threat to businesses in 2022,** with criminals not only asking for a ransom to be a paid but potentially then stealing and releasing hacked data too. It's vital that all organisations have fit and proper security systems in place to mitigate the threat as much as possible.

Text and cold-calling scams

The surge in the volume of scams taking hold in the UK shows no signs of abating in 2022.

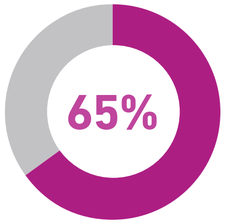
More than

£4 million

a day on average stolen in the first half of 2021 as people were tricked into handing over their cash.

These scams range from the sophisticated to the relatively simple but they all pray on a person's anxieties. Receiving a cold call or text message purporting to be someone from a genuine organisation asking you to authorise a payment relies on the victim to be panicked into action and handing over their personal information or agreeing to transfer money.

Digital payments fraud



A survey of UK consumers by Experian found 65% are now using a universal mobile wallet to make digital payments. But this increase in activity presents an opportunity for fraudsters to create accounts using stolen details to accept and transfer illegally obtained funds.

It's critical that businesses know who they are dealing with. Establishing that the person behind each transaction and interaction is who they say they are and using it for genuine means will only become more important as the levels of online activity continue to soar.

Though a small proportion of the level of overall fraud, the rise in the contactless limit from £45 to £100 could also lead to more people becoming a victim if their mobile phone or card is lost or stolen.

Cryptocurrency scams

Ransomware attacks

Text and cold-calling scams

Digital payments fraud

Social media oversharing

Changing fraud profiles

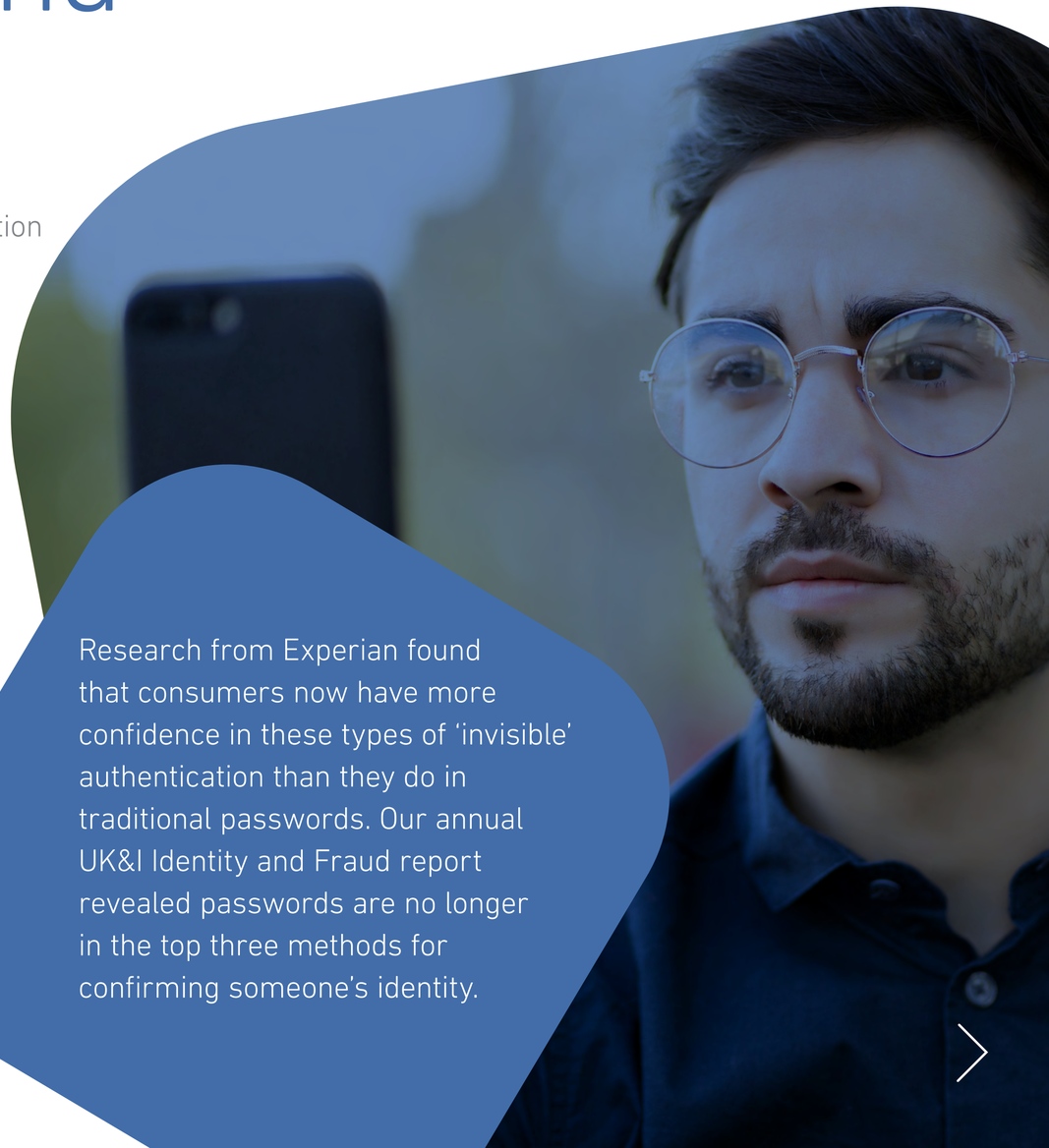
Social media oversharing and new ways of authentication

Simple passwords are likely to become increasingly obsolete. Fraudsters are clever at extracting information from people oversharing information on social media – such as birthdays, other dates or children's names - can lead to accessing and taking over victims' accounts.

This means passwords and traditional Knowledge-based Authentication (KBA) such as answering what your mother's maiden name is, are not as fool-proof as a means of verifying identity as they used to be.

New forms of authentication will continue to be used

PIN numbers sent to a person's mobile phone have become typical, while biometrics systems – both physical and behavioural – are becoming more familiar and accepted by consumers and organisations.



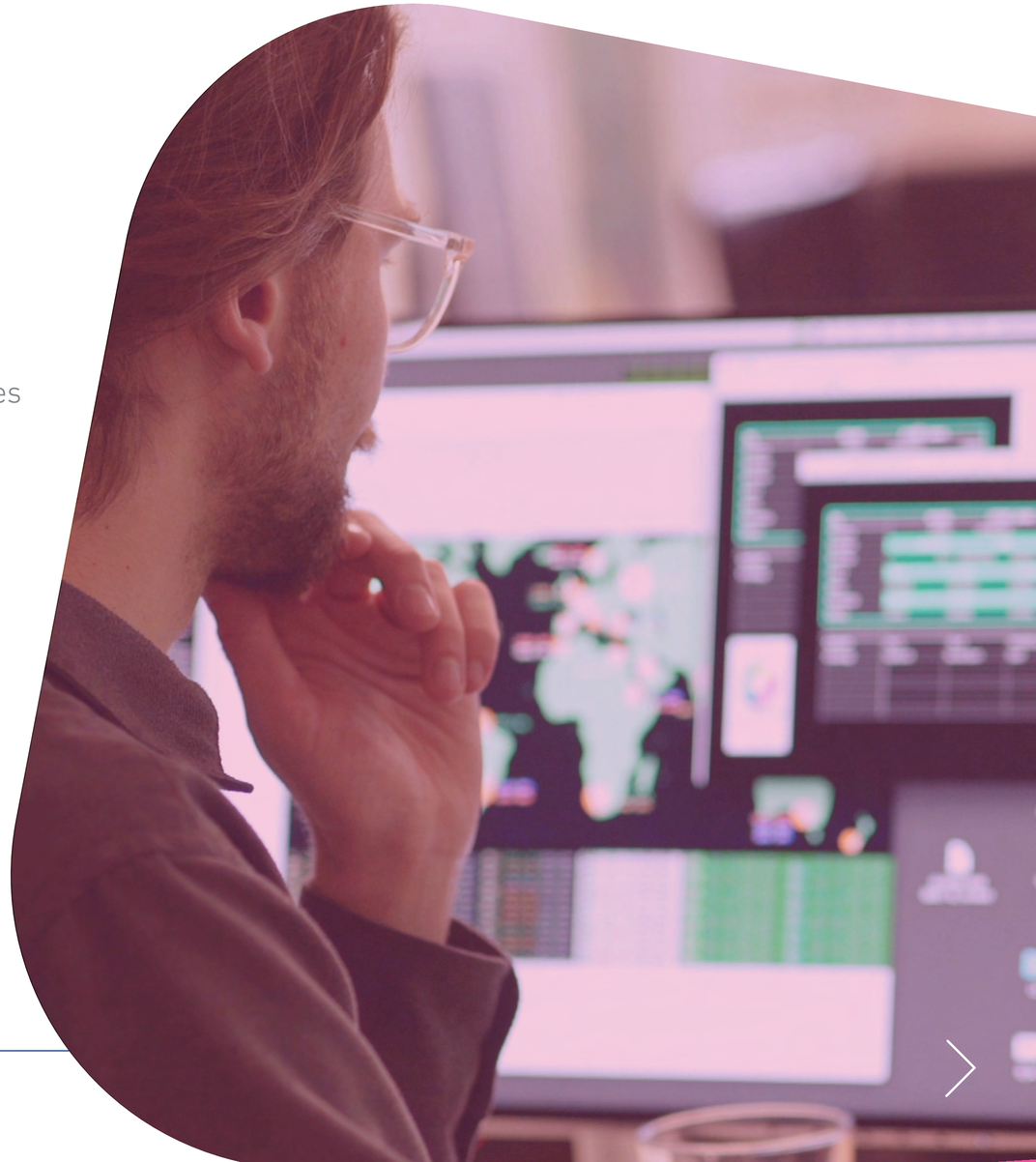
Research from Experian found that consumers now have more confidence in these types of 'invisible' authentication than they do in traditional passwords. Our annual UK&I Identity and Fraud report revealed passwords are no longer in the top three methods for confirming someone's identity.

Changing fraud profiles

Changing economic circumstances could mean financial services companies see customers with already opened accounts commit fraud when otherwise they wouldn't have done.

Two types of fraud are happening in this way. **Bust-out fraud** – where individuals take out an account to ease financial pressures with no intent to repay – and **first-party account fraud** where a customer falsifies information on an application to access more borrowing or favourable terms.

With fraud profiles ever-changing, it's critical businesses assess whether their current systems are effective in identifying this type of fraud. Regularly checking already opened accounts offers the chance to identify new information which could have flagged fraudulent activity at the point of application.



Conclusion

More than ever, both businesses and consumers need to be aware of the threat posed by fraudsters. People should do all they can to ensure their personal information isn't compromised and businesses must prioritise their fraud prevention systems, making sure they are robust and fit for purpose.

If they don't, they risk serious reputational damage, with customers choosing to look elsewhere online for companies which they do trust to handle their information in a safe and secure way.

Cryptocurrency scams

Ransomware attacks

Text and cold-calling scams

Digital payments fraud

Social media oversharing

Changing fraud profiles