SHINING A SPOTLIGHT ON THE LATEST FRAUD TRENDS

2023 UK Identity and Fraud report

Contents

INTRO

How are businesses and consumers reacting to a changing fraud landscape?

Introduction

2023 is proving to be another year of challenging economic conditions in the UK, with high inflation and rising energy prices squeezing consumers' household budgets. But in spite of these pressures, the vast majority are following the rule of law and making use of credit products in a legitimate way to maintain their lifestyles and comply with their payment obligations.

However, one inevitable impact of the growing inflationary period has been a significant increase in certain types of financial behaviour and, in particular, fraud.

Specifically, Experian data from late 2022 into 2023 shows a marked increase in first-party fraud, mostly associated with asset finance, loans and mortgage applications. Likewise, there is an upward trend in Application Push Payment (APP) fraud, including everything from fake investment schemes to romance scams, over this period.

Against this backdrop of increasing, and ever more complex fraud risks, several key questions arise. For example:

- How are businesses ramping up their investments to tackle the growing fraud challenges?
- Which technology solutions are organisations developing and implementing to identify and authenticate consumers accurately and reliably online?
- How are consumers' expectations evolving in terms of security and convenience in the online journey, and are organisations' identity and fraud-prevention capabilities keeping pace?

The Experian 2023 UK Identity and Fraud Report provides some answers to these and other questions – giving organisations a clear view of current progress on fraud prevention and shifting consumer expectations, and helping to steer future investments.

Key topics for this year's report are:

- The evolving fraud landscape, shifting regulations and the impacts for organisations
- How consumers are demanding more in terms of fraud prevention, and how organisations are responding
- Why Machine Learning (ML) is now an essential component of any effective fraud strategy

About the **Experian research**

The Experian Identity and Fraud Report for 2023 is based on two major surveys, conducted in the UK. The first asked more than 2,000 UK consumers about their online interactions and their expectations with regards to security and customer experience.

The second survey asked more than 200 UK businesses about their strategies for effective fraud management and customer identification and authentication, including investments in new security and customer-experience related technology solutions. Organisations surveyed for the research include retail banks, fintech organisations, digital retailers, electronics providers, payment providers, and many other companies from a range of verticals.

1 How the evolving fraud landscape and new regulations are impacting UK organisations and consumers

Report highlights

Businesses are increasingly concerned about fraud risks especially Authorised Push Payment (APP) fraud, Account Takeover fraud and First-party fraud

69% of organisations report fraud losses are '**significantly or somewhat**' higher compared to the previous reporting year

35% of UK consumers feel like they are '**more of a target**' for online fraud than a year ago

The most common fraud types encountered by organisations last year were:

1. APP fraud & money mules – **54%**
2. Transaction fraud – **38%**
3. Account takeover fraud – **38%**
4. First-party fraud – **36%**
5. Synthetic fraud – **30%**

Market context

The cost-of-living crisis in the UK drove a significant increase in first-party fraud in the last quarter of 2022. In particular, card fraud increased significantly during this period, along with fraud associated with asset finance and loan applications. However, the greatest jump in fraud cases has been seen in the mortgage market, with fraud increasing from around 41 cases to around 52 cases per 10,000 applications.[1]

This all points to a trend of consumers providing inaccurate information to support their applications. To reduce the negative impacts of this kind of fraud, organisations need advanced, data-driven solutions that cross reference customer applications with open-banking data, credit bureau data and other sources that can verify customers' financial situations and indicate the possibility of fraud before losses are incurred.

Preparing for new UK APP legislation

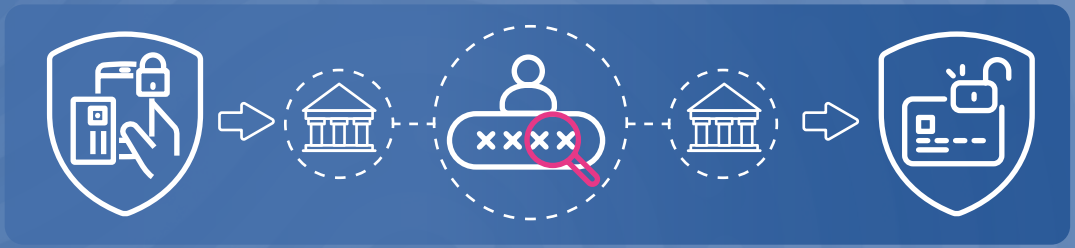
Legislative changes, such as the Financial Services Markets (FSM) Bill, are a key trend impacting lenders in 2022-2022. The FSM Bill, will require Payment Service Providers (PSPs), rather than consumers, to pay for losses related to Authorised Push Payment (APP) fraud.

APP fraud involves a fraudster persuading a victim to willingly deposit funds to their account, or – far more commonly – to the account of one or more complicit third parties (money mules). APP fraud often includes social engineering of the victim using fake investment schemes, impersonation scams, purchase scams, or other such schemes.

The Payment Systems Regulator (PSR) reports that there are more incidents of APP fraud than any other type of fraud in the UK, with 95,219 incidences in H1 2022, with gross losses of £249.1 million.

[1] https://www.experian.co.uk/blogs/latest-thinking/fraud-prevention/quarterly-fraud-index-report/

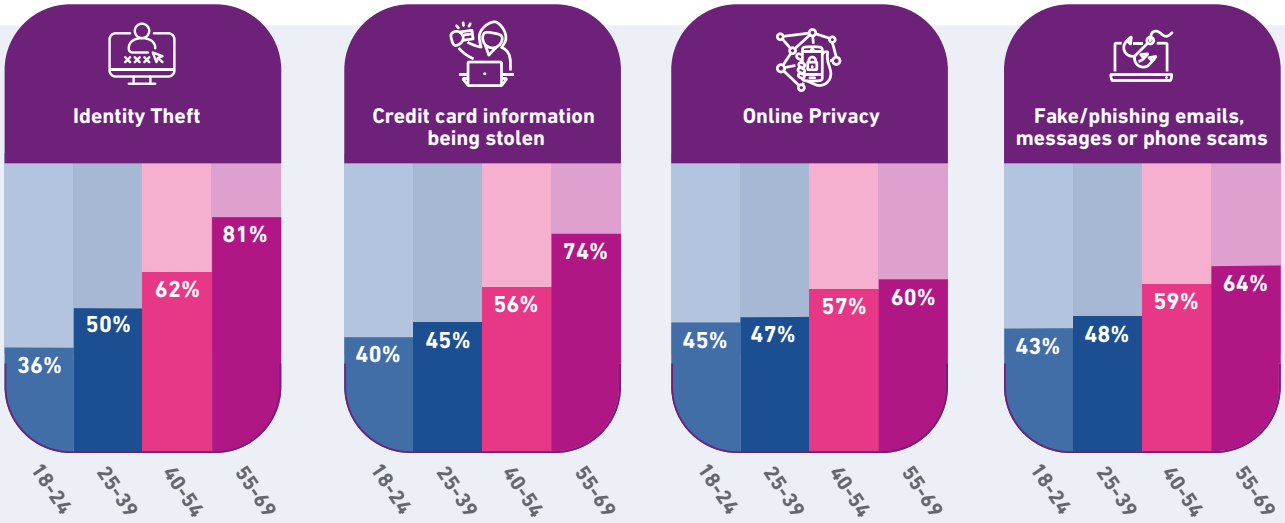
To address the growing challenges of APP fraud – and to minimise liability related to the new FSM Bill – **organisations are implementing the Confirmation of Payee (CoP) system, which allows the payer bank to check that the payee name entered by the payer matches the name on the recipient bank account before the transaction is authorised.** However, other technologies – such as advanced analytical models, behavioural biometrics, device intelligence and real-time transaction monitoring, can also significantly reduce risk factors related to APP fraud.



Consumer viewpoint

This year's research shows that consumers are most concerned about online identity theft (58%), followed by their credit card information being stolen (53%). However, fake and phishing emails, false information, crypto scams and romance scams – which all potentially fall under the category of APP fraud – are all strongly represented as pressing consumer concerns.

Table 1: Consumer concerns by fraud type and age category



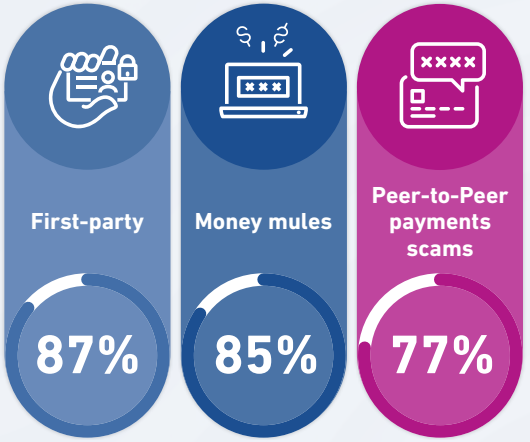
The research also reveals the primary fraud types are of highest concern in the older age categories, most notably, 81% of 55-69 year olds are concerned by Identity Theft

Business viewpoint

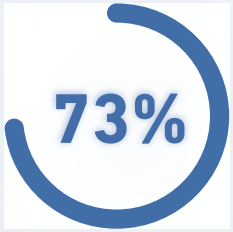
While 53% of organisations have a high level of concern about fraud risks, this year's report indicates the majority of businesses have confidence in their ability to protect against fraud.

However, this confidence doesn't mean businesses are standing still on fraud. Growing first-party fraud and APP fraud are driving investments in next-generation identity and fraud-prevention technologies.

Organisations' level of confidence in their ability to protect against fraud.



Businesses are ramping up their fraud-prevention efforts in the face of growing first-party and APP fraud challenges



of businesses are expecting increased budgets for fraud management. Of these, **79%** are expecting increases of more than **8%**, with **6%** expecting increases of **20% or more**

of businesses are planning to implement additional security measures for online authentication, often requiring customers to have a 'device in hand' to confirm their identity

Experian viewpoint

Organisations and consumers are aligned when it comes to their concerns about growing fraud risks. For businesses, however, growing first-party fraud risks, and new UK legislation that makes institutions liable for losses associated with APP fraud, require fresh approaches that support real-time transaction analysis and enhanced end-user identification and authentication.

2 How consumers are demanding even more action from organisations on identity and fraud

Report highlights

Businesses' identity and fraud measures may not be keeping pace with consumer expectations

Security and fraud
(consumer expectations vs. reality)

Consumers' most trusted security methods are:

73% Physical Biometrics

73% Behavioural Biometrics

71% Mobile PIN Code

However, neither physical nor behavioural biometrics are in the top technologies knowingly encountered during online account opening processes.

1. **86%** PIN
2. **81%** Passwords
3. **77%** Security questions
4. **72%** Account name

Market context

Despite increasing budgets for fraud prevention, organisations' current capabilities are still struggling to keep pace with consumers' fast-changing expectations. This is brought into sharp focus by consumers' views on physical biometrics, for example, which is the most trusted authentication method for 73% of people, but which is only currently knowingly encountered during 21% of new account opening processes.

More evidence of this is the fact that passwords, security questions, account usernames and contact information are all in the top-5 list of methods currently used for account opening processes. However, only one of these methods (security questions), features in the list of consumers' most-trusted solutions.

Instead, organisations are planning to ramp up investments in security measures that require customers to have a 'device in hand' (41%). Almost as many (34%), will also be investing in behavioural biometrics-type solutions that look at anomalies in customer behaviour, spending patterns and transaction histories to identify fraud.

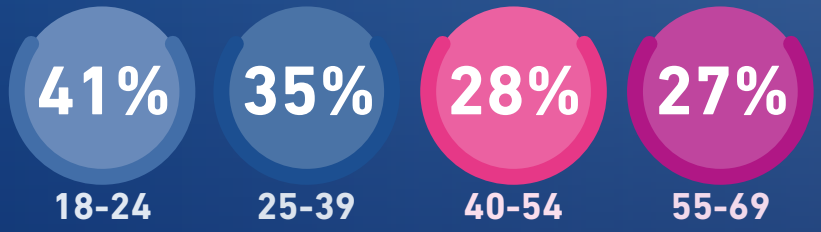
Another key investment priority is physical biometrics, with a third of UK companies (33%) planning to add this kind of solution to their identity and fraud prevention strategies. Interestingly, 30% of organisations also plan to add Captcha or other image-based solutions in 2023. This shows that the risks associated with denial-of-service (DDoS) attacks is still real and present for businesses across the UK.

Unhappy consumers vote with their feet

The gap between consumer expectations and current identification and authentication methods is having a significant and measurable impact on abandonment rates in new account opening processes.

In particular, 32% of UK consumers have considered abandoning a new account opening journey due, for the most part, to the onerous nature of the information requested from them (rising to 41% in the 18 to 24-year-old age category).

Proportion of consumers who have considered abandoning account opening by age.



At the same time, a fifth of UK consumers have acted on this urge and taken their business elsewhere because of a sub-optimal online experience, or because of concerns about online security.

Nearly 48% of UK consumers have set up a new account in the last six months, with the most common accounts relating to streaming services (28%), branded retail apps (27%), and payment system provider accounts (25%).

Consumer viewpoint

It's clear that consumers' have exacting expectations when it comes to service providers' obligations to provide secure online experiences – and also for the kinds of technologies and experiences they consider optimal. However, the seeming mismatch between consumers' wish lists for online identification and security – and the experiences they encounter in the real world – are leading to reduced satisfaction and increased abandonment during new account opening processes.

Business viewpoint

These findings, more than any other aspect of the 2023 report, demonstrate the scale of the challenges faced by businesses in terms of optimising their identity and fraud-prevention strategies. While some key investment priorities – such as physical biometrics – are totally in line with consumer preferences – each organisation needs to carefully review its strategy to ensure that investments in new identity and fraud solutions can minimise abandonment rates and other measures of consumer dissatisfaction whilst simultaneously achieving fraud prevention targets.

The most trusted businesses – by segment

Our research shows that retail banks and payment system providers (PSPs) elicit trust from the highest percentage of UK, with tech companies and telecommunications providers also performing well:

1. **27%** Retail banks
2. **23%** Payment system providers
3. **22%** Streaming services
4. **20%** Tech providers

Experian viewpoint

The 2023 report indicates that customer expectations are moving extremely quickly and that organisations who can keep up will be able to achieve new competitive advantage and deeper levels of market trust. However, achieving this will require targeted investments in ML-driven technologies that can significantly improve online security and customer experiences, as well as prioritisation of the security technologies that consumers trust most: namely, physical and behavioural biometrics.

When it comes to online identification, consumer and business expectations seem to be well aligned.

For example, 89% of organisations have a strategy in place for identifying consumers online, and 83% are confident in their ability to achieve it – up from an average of 76% last year. At the same time, 97% of consumers say they are confident or somewhat confident that their providers can identify them online (of which 14% are very confident and 83% are somewhat confident).

Effective online identification is seen, by consumers, as a major benefit, both in terms of reducing fraud risks, and for improving the speed and convenience of online transactions and other customers experiences.

So much so, in fact, that 83% of consumers are 'somewhat trusting', 'very trusting' or 'extremely trusting' towards providers who can reliably and accurately identify them online.

3

Why Machine Learning is no longer a ‘nice to have’ for fraud prevention

Report highlights

ML is becoming mainstream as a fraud-prevention method, and cost is the biggest perceived barrier to adoption

35% of businesses are planning to add Machine Learning capabilities to their online security portfolios to **minimise fraud risks**

49% cost is deemed the main barrier to ML adoption according to **almost half** of organisations

Market context

A large majority of organisations still use rules-based analytics models to identify and flag incidences of suspected fraud. However, with fraudsters continually innovating and perpetrating new types of attacks, static models quickly become obsolete, increasing the risk of fraudulent transactions, data breaches, and regulatory non-compliance – not to mention costs associated with these.

To address all of these issues in 2023, more than a third of organisations are looking to build ML capabilities into their fraud identification and prevention strategies. ML is far superior to rules-based fraud models the technology identifies both known and unknown trends in large datasets. When a new fraud trend or type emerges, the ML model is able to identify it and flag it to the security team immediately for further investigation.

The other benefit of ML is that large numbers of transactions or large datasets can be analysed automatically, extending fraud prevention measures across the entire customer portfolio. This ensures that new and existing fraud risks can be identified quickly and at scale, and that legitimate customers can continue transacting with their providers reliably, helping to enhance their online experiences.

In the 2023 report, 35% of organisations said they are planning to add ML to their fraud-prevention toolsets. However, a large percentage of businesses (49%), also cited cost as the most significant barrier to ML adoption. This suggests that many still have their ML plans on hold as they wait for more cost-effective solutions to come to market.

This delay is potentially worrying, particularly as traditional models are now incapable of keeping pace with evolving fraud threats. What's needed is a new generation of more cost-effective fraud solutions that have ML as a natively integrated component.

Consumer viewpoint

As we have seen, security and privacy rank as consumers' top concerns in 2023. Not only that, but 89% say it is important for online businesses to accurately identify them online. Based on its ability to automate and enhance both fraud detection and online customer identification, ML has now become an essential technology for organisations wishing to keep pace with consumers' growing security expectations.

Business viewpoint

With more than a third of companies planning to add ML-powered solutions to their identity and fraud portfolios, it's clear that the power of this technology to detect and prevent fraud is now well understood across all markets. However, cost is seen as a major barrier to adoption, suggesting that many companies are still putting their ML plans on hold.

Experian viewpoint

Experian has long understood that ML will be a key technology for helping organisations to recognise and respond to both existing and new fraud threats. To make ML capabilities available to organisations in all verticals, we have built ML into a number of our fraud prevention and data analytics solutions, dramatically reducing costs and ensuring that our customers can access fully trainable models that deliver accurate, timely fraud insights across their portfolios.

When it comes to detecting and preventing fraud, advanced analytics, like machine learning, is now a non-negotiable. Incorporating machine learning fraud models leads to a simplistic, more understandable referral strategy, which equates to less manual referrals, more straight through accepts and a reduction in false positives.

Eduardo Castro
Managing Director, Identity and Fraud, Experian UK

4 How Experian can help

How Experian can help

As we continue to see higher incidences of first-party and all types of APP fraud, organisations are significantly increasing their investments. At the same time, almost all organisations are pursuing their online identity strategies to ensure that all customers can be identified and authenticated quickly, accurately and conveniently, all of the time.

But this year's report also highlights a gap between consumers' expectations for even more online protection and convenience, and organisations' ability to act, and innovate, quickly enough. In particular, greater investments are needed in the security technologies consumers trust the most – including physical and behavioural biometrics. Additionally, organisations will need to continue and expand their investments in ML-driven solutions that can detect and prevent emerging, as well as new fraud threats in real time.

As organisations strive to keep pace with the evolving fraud landscape, and to deliver even more convenient, frictionless online experiences for consumers, Experian can help.

How Experian can help

1 Get a single view of fraud risks and act quickly to mitigate them

This is possible thanks to our end-to-end integration, orchestration and analytics capabilities, which give you real-time alerts for fraud risks, while ensuring that your legitimate customers can transact with you safely and reliably. As well as reducing fraud risks, this can help you to provide a more streamlined, unified customer experience that minimises abandonment during the onboarding process.

2 Prepare for upcoming regulations – specifically around APP fraud

At Experian, we offer the rich data sources, advanced analytics capabilities, and consultancy and services needed to rapidly adopt data analytics solutions that mitigate APP fraud risks. Our solutions are used by PSPs of all types and sizes – including some of the largest banks – to identify potentially fraudulent customers and transactions, and to ensure that action is taken in real time to prevent fraudulent payments being made.

3 Take full advantage of the fraud-prevention power of ML

We have built ML into CrossCore, our integrated fraud-detection platform, to ensure that you can identify both existing and emerging fraud trends quickly and easily, and prevent potentially fraudulent transactions before your business, or your customers, are compromised. Full integration of ML capabilities into our platform also reduces costs, helping to make these capabilities available to organisations of all types and sizes.

4 Educate customers to help them protect themselves online

We provide a wealth of data on your customers – and the wider UK consumer population – to help you understand their wants and needs and, critically, their level of comfort and knowledge when transacting online. Using customers' demographic data, you can understand them better, and – where appropriate – help to educate them about online security to help them protect themselves.

5 Double down on initiatives that build consumer trust

Establishing a track record of accurate recognition and secure online transactions with consumers increases the depth of the relationship. And the core of the relationship is trust. Elevating your authentication and security efforts in light of the continued increase in first-party fraud and APP fraud demonstrates that your business also values the relationship – and can help preserve it for years to come.

Organisations of all types and sizes work with Experian to maximise their fraud prevention and identity capabilities. In particular, our CrossCore platform can help you bring together a range of fraud, ID and authentication solutions to drive security and customer experience KPIs.

To discover more about our capabilities in this area, please **visit the website**. You can also contact us to discuss your specific security, fraud and identity requirements.

Registered office address:
The Sir John Peace Building, Experian Way,
NG2 Business Park, Nottingham, NG80 1ZZ

www.experian.co.uk

C-01754