Global Insights from Experian

Global Identity & Fraud Report 2024

Using business and consumer quantitative and qualitative research from the UK, US, Brazil, EMEA, and APAC between 2023 and 2024, we assess the current global impact of fraud.

Contents

Executive Summary

Experian's 2024 Global Identity and Fraud Report provides a comprehensive view and analysis of consumer and business sentiment towards the latest fraud patterns and fraud mitigation strategies in financial services worldwide.

Our research shines a light on the fast-evolving fraud landscape, driven by huge growth in generative artificial intelligence (GenAI) technologies, changing regulations, and the quest to provide consumers with secure and convenient digital experiences. As a result of the rise of GenAI, the personalisation and scale of fraud attacks have increased massively over the past 18 months.

Businesses are tasked with finding ways to address identity-related fraud, hugely impacted by fraudsters' ability to create authentic-looking deepfakes while abusing the latest advancements in technology to improve their social engineering tactics and their chances of penetrating companies' fraud defences.

Along with accessible GenAI tools, the prevalence of instant payment methods has accelerated Authorised Push Payment (APP) fraud, leaving financial institutions walking the tightrope between providing consumers with convenience and mitigating APP fraud effectively.

This, coupled with an increased focus on regulations that require financial institutions to reimburse APP fraud victims, means businesses must add effective protection for consumers fast.

Our findings reinforce the need for businesses to leverage advanced analytics, alternative data insights, data sharing, and a multi-layered approach to combat evolving fraud threats globally.

About the research

The 2024 Global Identity and Fraud Report uses the latest research from the United States, the United Kingdom, Brazil, EMEA, and APAC between 2023 and 2024 to examine fraud worldwide. The research provides combined insights globally from over 1,000 businesses and fraud leaders, as well as 4,000 consumers, focusing on fraud management and digital experience. See the appendix for full details of the research.

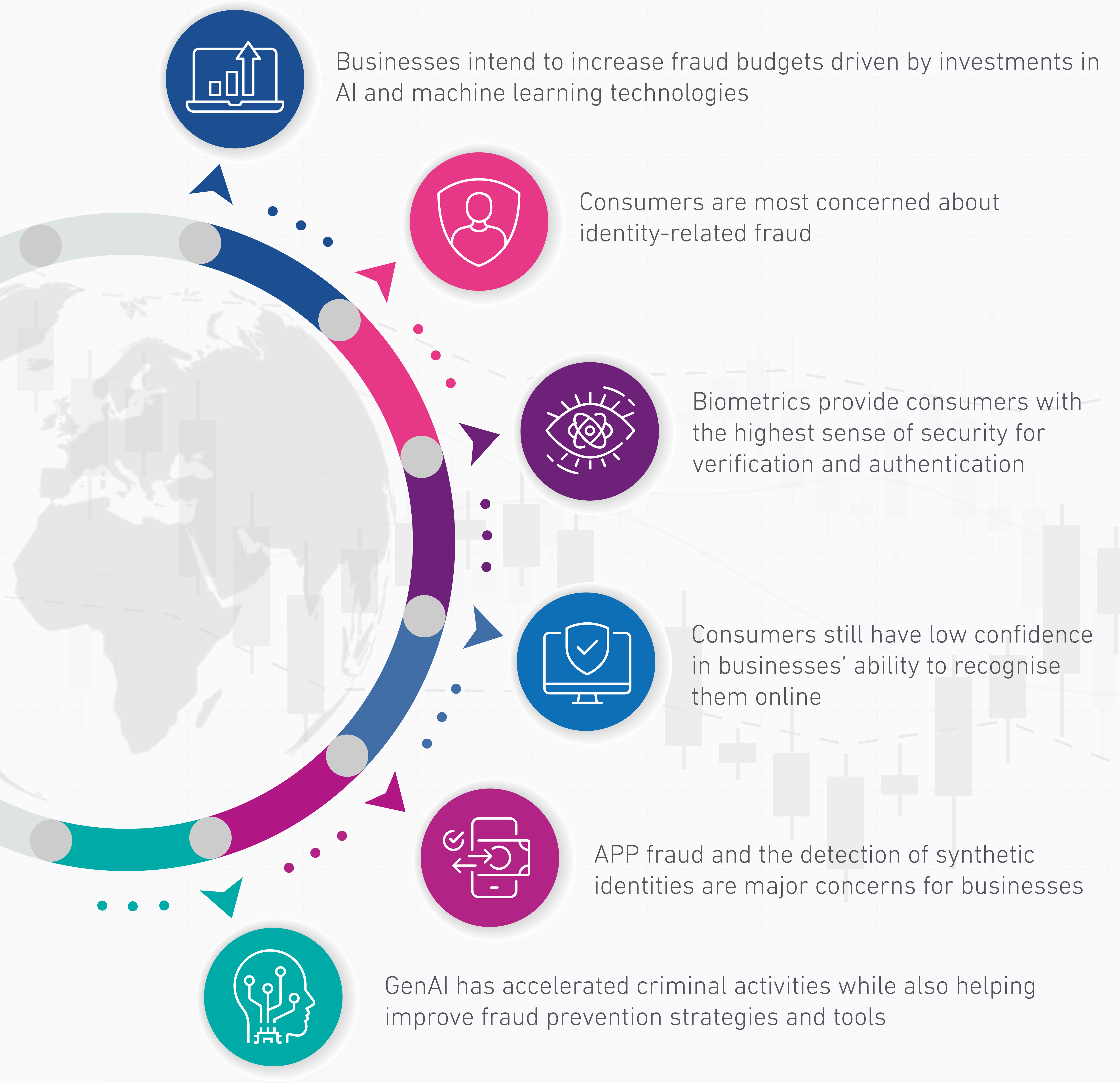
- Read Experian's 2024 U.S. Identity & Fraud Report
- Read Experian's UK Fraud and Fincrime Report 2024
- Read more from Serasa Experian, Brazil
- Read Experian's EMEA & APAC 2023 Defeating Fraud Report

Introduction

> Fraud knows no borders, posing a global challenge that necessitates unified action. Unlike some issues facing financial services, fraud operates beyond geographical boundaries or regulatory frameworks. While its impact may initially target specific locales, the source of the threat can emerge from distant corners of the globe, far removed from the victim's vicinity.
>
> Fraudsters do not simply attack one part of a business, but often seek to attack different points across the consumer journey. This requires businesses to evolve their approach to fighting fraud by leveraging a cross-enterprise view of activities while aggregating the tools and data necessary to create a holistic defence.
>
> Reflecting on global fraud trends allows businesses to take a comprehensive view of issues that may already be affecting their operations, while identifying the areas to invest in to mitigate fraud threats in the future.

Greg Wright,
Executive Vice President of Identity & Fraud,
Experian

Key insights unveiled in this year's report



Businesses intend to increase fraud budgets driven by investments in AI and machine learning technologies

Consumers are most concerned about identity-related fraud

Biometrics provide consumers with the highest sense of security for verification and authentication

Consumers still have low confidence in businesses' ability to recognise them online

APP fraud and the detection of synthetic identities are major concerns for businesses

GenAI has accelerated criminal activities while also helping improve fraud prevention strategies and tools

Economic uncertainty and the emergence of new technologies

Economic uncertainty has been a persistent issue for some time, and the past year has been no exception. Globally, businesses and consumers grappled with high inflation, rising interest rates, and increased living costs, which strained consumer spending and business investment. Additionally, advancements in technology have opened new avenues for fraudsters to exploit.

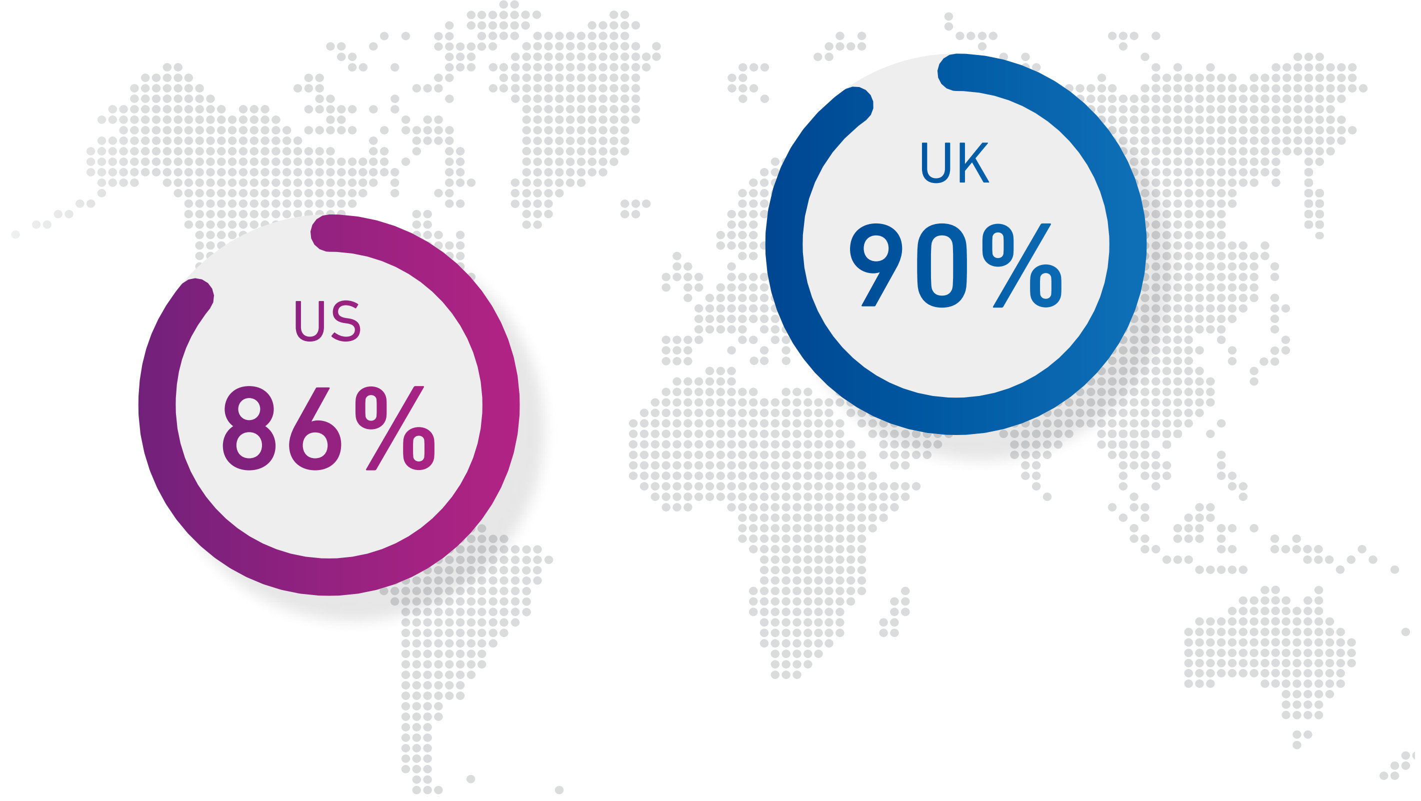
The World Economic Forum cites AI-generated misinformation and disinformation as the second biggest global risk of 2024. The exponential growth of GenAI has lowered the entry barrier for criminals, allowing them to launch highly personalised fraud attacks on an unprecedented scale. This surge has led to a wave of identity theft and synthetic identity fraud while also fuelling APP fraud by arming fraudsters with new abilities to commit convincing social engineering at scale. Our research reflects this shifting landscape, revealing that consumers are most concerned about identity theft when it comes to online activities. Meanwhile, businesses report that detecting and preventing identity theft and synthetic identity fraud are among their greatest sources of stress.

In response, businesses seek to mitigate these risks by increasing their investments in fraud prevention with a focus on AI. Our research shows that businesses increasingly recognise how AI and machine learning can be effective tools within their fraud prevention solutions, showing early confidence in GenAI solutions already in use.

In addition, the normalisation and acceleration of digital payments, driven by rapid technological advancement, have provided criminals with new ways to exploit victims. According to Juniper Research, losses from online payment fraud could exceed $362 billion globally by 2028. As organisations around the world report rising fraud losses, businesses are increasing their fraud prevention budgets, and prioritising high-risk areas such as APP fraud, transactional payment fraud, identity theft, and synthetic identity fraud.

This challenge is further compounded by regulatory pressures from governments aiming to curb the surge of fraud in real-time payments (RTP) and peer-to-peer (P2P) payments. Recent evidence includes US congressional inquiries calling for major banks to explore enhanced consumer protections against fraud, including the implementation of cross-industry solutions.

Business confidence levels in GenAI solutions currently used to detect and protect against fraud



Acceleration of digital payments

UK

Use of **mobile wallets** has surged from 54% to **77%** in the last two years.

Retail apps are used by **76%** of consumers compared with 36% two years ago.

More than eight in ten shoppers have embraced **P2P payment apps.**

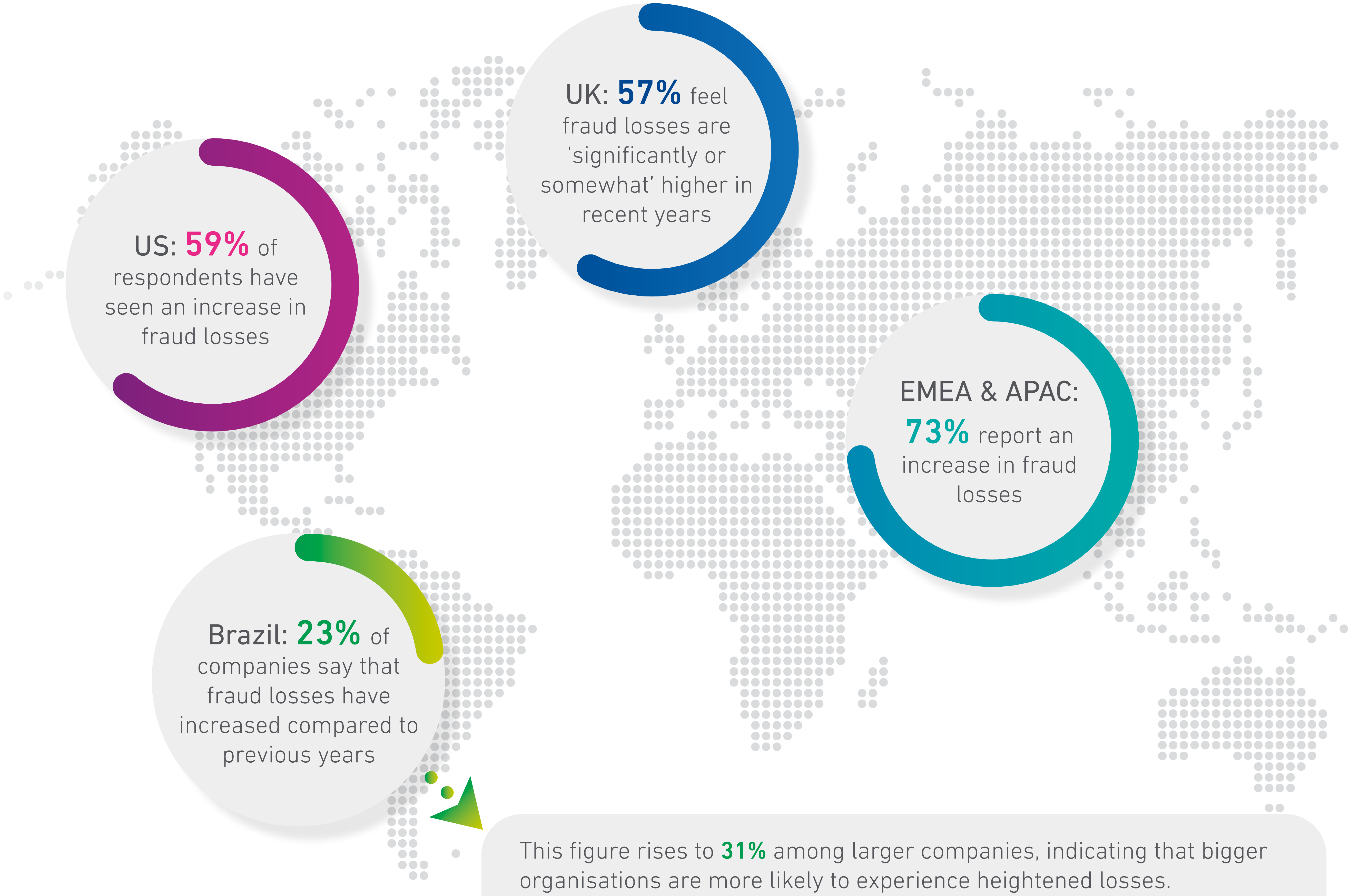
US

Mobile wallets usage increased by 12% up to **73%** over the past year.

Adoption of **retail apps** saw the highest growth, with usage rates rising from 51% in 2023 to **81%** in 2024.

P2P payment apps boast the highest usage with more than eight of ten shoppers relying on them.

Businesses are experiencing a continued increase in fraud losses



UK: **57%** feel fraud losses are 'significantly or somewhat' higher in recent years

US: **59%** of respondents have seen an increase in fraud losses

EMEA & APAC: **73%** report an increase in fraud losses

Brazil: **23%** of companies say that fraud losses have increased compared to previous years

This figure rises to **31%** among larger companies, indicating that bigger organisations are more likely to experience heightened losses.

58% of companies express greater concern about fraud compared to the previous year.

How businesses are approaching fraud management

Concern about fraud has led to increased budgets for fraud management in the UK, US and Brazil

UK

70% of businesses expect their budgets to increase even further.

In 2024, businesses plan to increase investments, with a primary focus on implementing and enhancing AI models to improve customer decisions (**63%**) and prevent APP fraud (**61%**).

US

Around **three-quarters** of US businesses intend to increase their fraud management budget.

Businesses are primarily engaged in improving and building new AI models that address non-customer decisions (**60%**) and prevent APP fraud (**60%**).

Brazil

Companies are investing more in fraud prevention (**46%**) than the previous year.

65% of large companies are increasing their investment in fraud prevention, with 35% reporting significantly higher spending.

EMEA & APAC

71% of respondents struggle to keep up with the rapidly evolving fraud threat.

74% of respondents believe that ML-based fraud detection is the most effective way to prevent fraud.

Economic pressure contributes to a rise in first-party fraud occurrences. In EMEA and APAC, 59% of eCommerce merchants have experienced increased friendly fraud attacks. This is likely a direct result of ongoing financial pressure on consumers. Simultaneously, two-thirds of UK businesses report that their primary focus is on preventing first-party fraud.

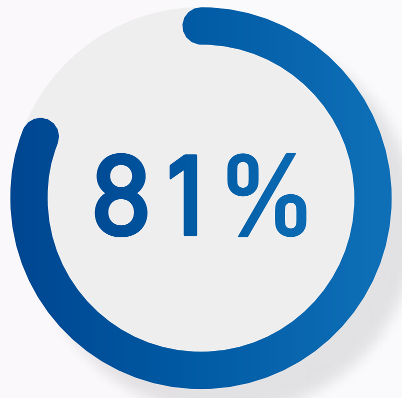
Consumers show concern about identity-related fraud

Consumers worldwide are more aware of fraud threats than ever before, yet the sophistication of fraudsters' tactics can still deceive even the most informed digital natives.

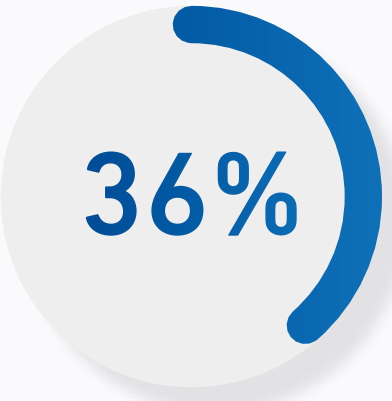
Our research shows that consumer attitudes towards fraud vary based on location. In the US, **39%** feel increasingly targeted by online fraud compared to a year before, while in the UK, this number is lower at **36%**. In addition, **51%** of US consumers say they are concerned about online security, with **11%** very concerned. In contrast, only **5%** of UK respondents are very concerned. However, awareness of fraud risk is high in the UK, with **81%** of consumers saying they are aware of online scams.

Differences in regulatory environments likely influence consumer attitudes toward fraud protection. In the UK, recent legislative changes—including mandatory reimbursement, public data reporting, and enhanced intelligence sharing through the Financial Services and Markets Bill—may play a role in shaping consumer perceptions of fraud threats.

Consumers in the UK show signs of feeling protected from online scams but remain vigilant



say they are aware of online scams

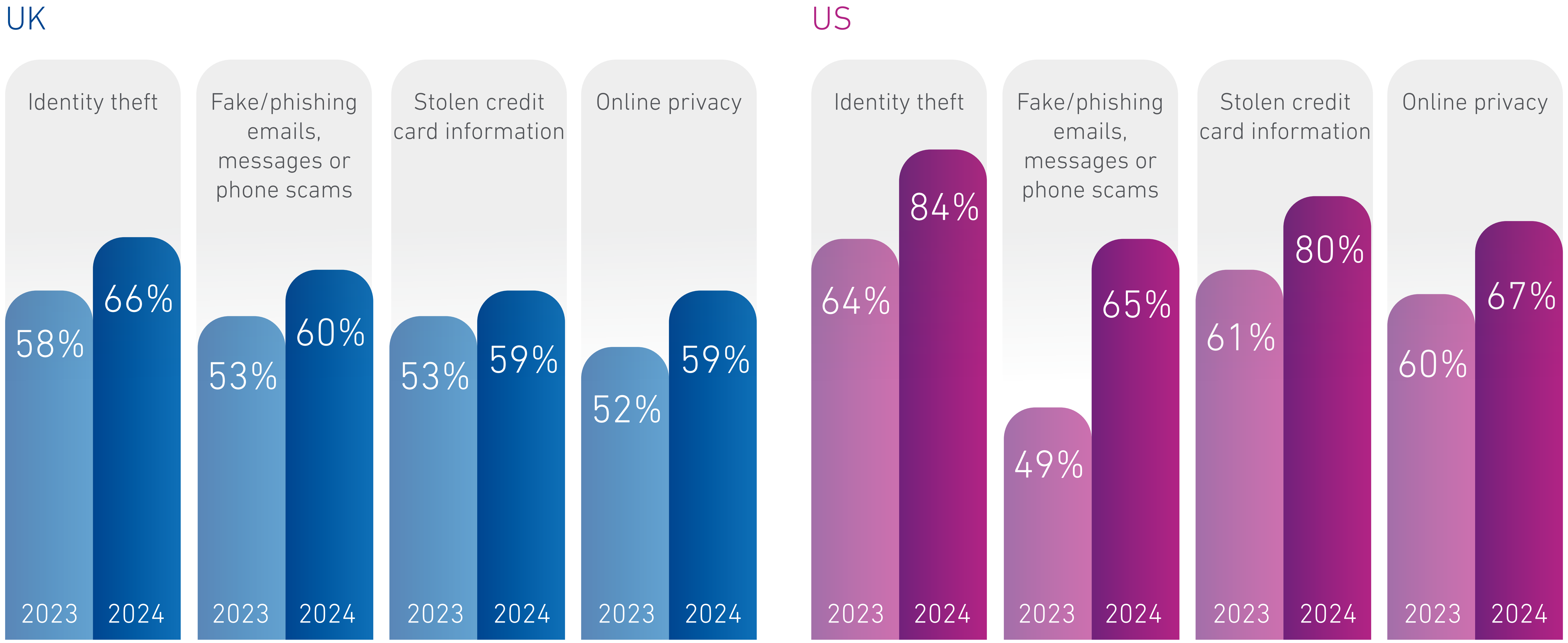


say they are concerned about online security

In Brazil, **71%** of people say they are concerned about online security and identity theft, citing online shopping security (**88%**) and privacy (**87%**) as the most important dimensions. Identity theft is the top concern in the UK (**66%**) and the US (**84%**). In the UK, concerns increase with each successive age group, peaking among individuals aged 55-69. In this group, **80%** are concerned about identity theft and **76%** about phishing/phone scams. This age group is also the most worried about all four top-rated types of fraud in both the UK and the US.

As consumers become more active online, with a surge in the use of retail apps, mobile wallets, and P2P payments, they engage in various daily online financial activities. However, this increase in online activity also brings heightened awareness of the risks associated with their digital lives.

The top four online concerns for UK and US consumers have remained consistent, but the levels of concern have risen



Are businesses addressing concerns in the way consumers expect?

Given that identity theft is a key concern for consumers, it's not surprising that they view physical and behavioural biometrics as the safest identity verification methods. Organisations increasingly recognise the tangible value of verification methods such as biometrics to consumers. However, research indicates that many are still relying on authentication methods like one-time passcodes. Behavioural biometrics and its close counterpart, device intelligence, are passive identification methods that can significantly benefit businesses aiming to drive growth safely.

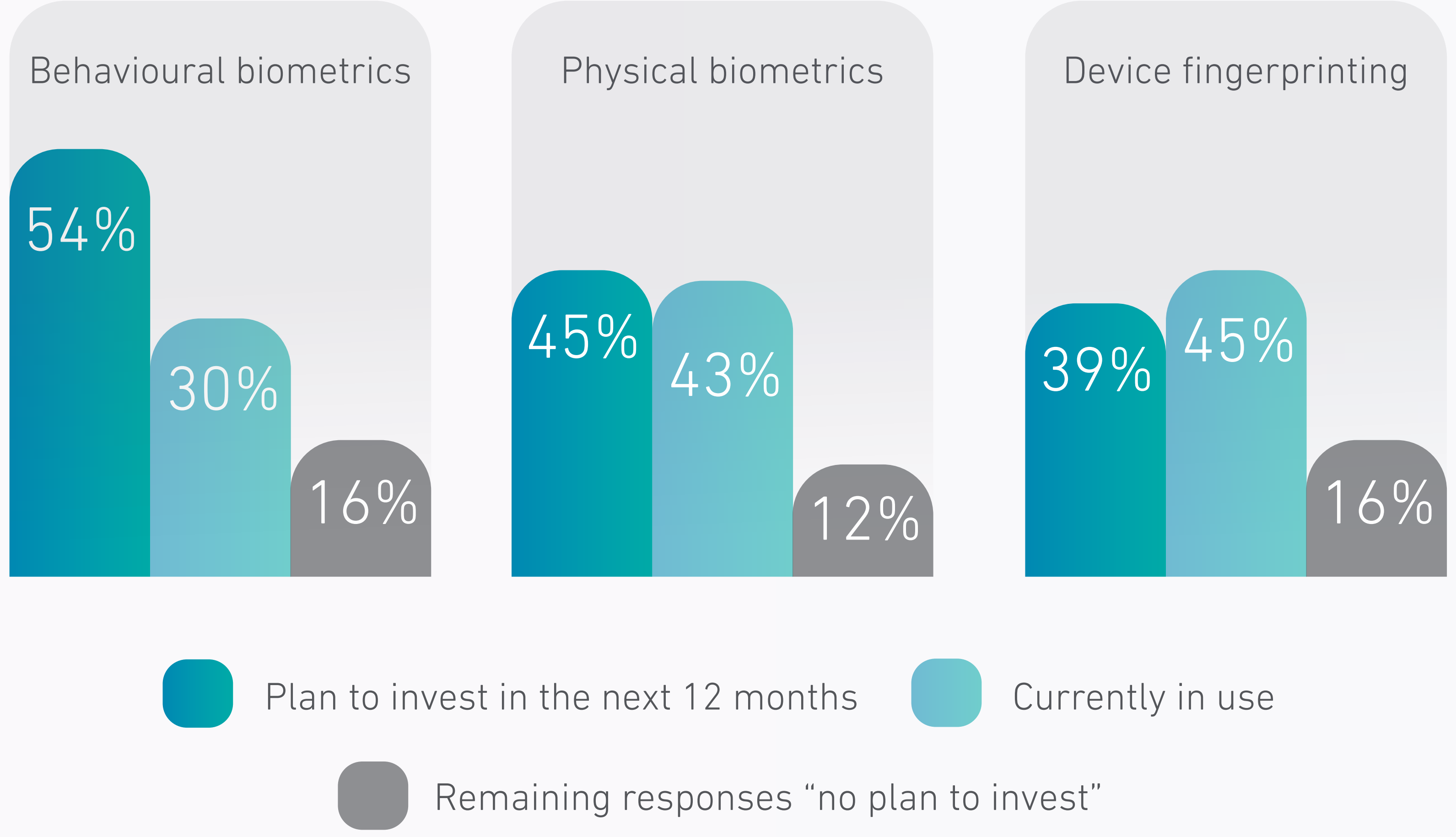
The online authentication methods that make consumers in the UK feel most secure are physical biometrics (75%), PIN codes (72%), and security questions (61%). High-income consumers express much higher-than-average feelings of security about behavioural biometrics, rating it higher than PIN codes or security questions (84% Physical biometrics, 82% Behavioural biometrics, 80% PIN code sent to device).

In the US, among the methods used most recently, physical biometrics (71%), PIN codes sent to a mobile device (70%), and behavioural biometrics (66%) evoke the highest sense of security for consumers. Similarly to the UK, in high-income households, physical and behavioural biometrics share the top spot for a sense of security among consumers at 78% each.

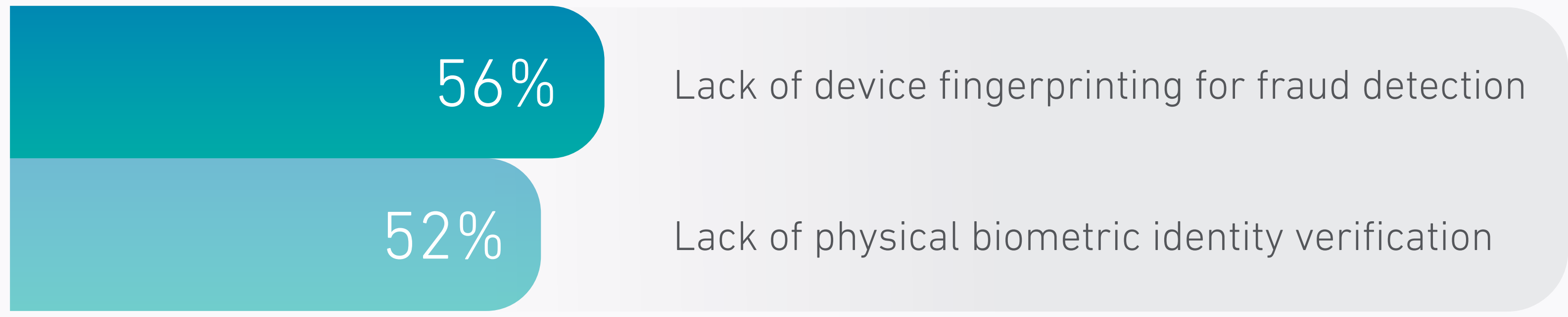
In Brazil, physical biometrics such as fingerprints, facial patterns, and voice are the method consumers feel most secure using, with 67% reporting they feel very secure or secure.

EMEA & APAC

Snapshot of current and future fraud prevention measures



Top challenges limiting businesses' ability to prevent fraud



In EMEA and APAC, 77% of businesses view biometrics as the most effective way to verify customer identity, and they plan to invest even further. Additionally, 73% of business respondents here think device fingerprinting is a must-have component of fraud prevention.

In the US, behavioural biometrics (96%) and physical biometrics (94%) ranked highest in businesses' confidence that their security investments align with customer preferences. Similarly, in the UK, physical biometrics is the top solution businesses plan to invest in for customer authentication.

Brazil

Document verification is the primary method of authentication and prevention used (**49%** and **57%** for larger companies, respectively). Customer score analysis is the second most common approach, used by **36%** of companies.

Physical biometrics is the method used the most to confirm online identity at **55%**, followed by PIN codes (52%).

Experian perspective

Advanced technologies like facial recognition and retinal scans are essential components of any firm's verification and authentication strategy. However, in the age of GenAI and deepfake technology, they are no longer sufficient on their own. Combining solutions from various vendors without a cohesive integration and unified risk strategy can lead to significant challenges, including integration issues, inconsistent data, fragmented fraud insights, increased operational overhead, and the complexity of managing multiple solutions.

To enhance online consumer identification without unnecessary interruptions, businesses need to implement a comprehensive layered fraud prevention strategy that utilises various methods and frictionless technologies. Incorporating multiple passive technologies—such as behavioural biometrics, device intelligence, and phone intelligence—alongside advanced analytics enables continuous monitoring of consumer behaviour across the user journey. This holistic approach not only safeguards against tech-savvy fraudsters but also strikes a balance between privacy and security.

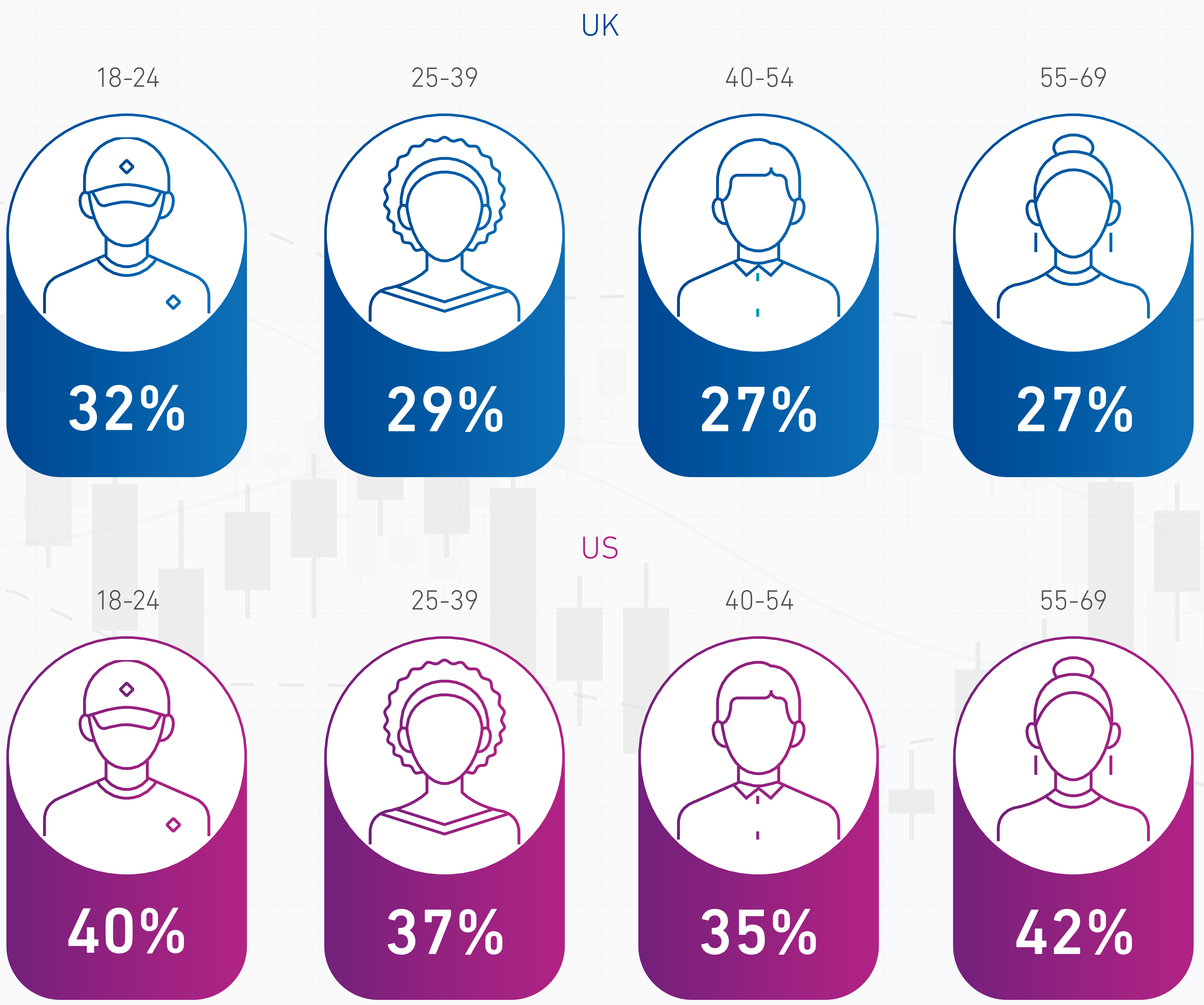
Advanced analytics is a powerful tool that every institution should consider adding to its arsenal against fraud. By leveraging vast datasets and sophisticated algorithms, businesses can identify fraud patterns, anomalies, and trends indicative of fraudulent activity.

Finding the right balance between fraud protection and a positive customer experience

While the gap between consumer expectations for online verification and the digital experiences businesses provide is narrowing, companies must not lose sight of the importance of customer experience and the critical role of identity verification and authentication across the customer journey.

In the UK, 16% of consumers report that they have moved their business elsewhere due to a poor account opening experience, while 28% considered halting a new account creation process because of their experience. In the US, nearly one-fifth of consumers have moved their business elsewhere, while 38% reported considering ending a new account opening mid-way through the process due to poor experience. In EMEA and APAC, 58% had abandoned an application during the previous year due to a lengthy, complicated process.

Percentage of consumers who considered stopping a new account opening process due to poor experience



Seamless digital identification is a consumer priority

For consumers, seamless identification during a digital experience is paramount. In Brazil, 69% of people believe it is extremely important for companies they deal with online to be able to accurately identify them. In the UK, 90% of consumers say it is important for businesses to be able to accurately identify or recognise them online on a repeated basis. However, only 11% have high confidence in businesses' ability to achieve this. In the US, 92% of consumers feel it's important for the businesses they deal with online to accurately identify or recognise them online on a repeated basis. Similarly to the UK, only 16% have high confidence that this is happening.

Reflecting consumer sentiment, our research in the UK indicates that business confidence in accurately identifying customers online is declining. While 83% were very or extremely confident they could do this in 2023, the proportion dropped to 68% at the start of 2024.

Authenticating customers requires balancing security and frictionless customer experience to prevent abandonment during applications or purchases—a challenge faced by businesses worldwide. In EMEA and APAC, 78% of business respondents believe that their fraud prevention strategies significantly affect customer abandonment rates, while only 20% consider the impact minimal.

of **EMEA & APAC businesses** believe their fraud prevention strategy impacts their customer abandonment rate

To truly understand customers in a digital-first environment, businesses must analyse vast amounts of interconnected information, including personal and alternative data. As they implement tools to mitigate fraud, an integrated view across multiple business lines becomes essential. Fraudsters often exploit gaps between these business functions, while legitimate consumers may experience friction in their journey due to a lack of cohesion.

Data is central to gaining a holistic consumer view, so how businesses communicate with consumers about the collection and use of personal data is pivotal in improving the digital experience. In the UK, only 21% of consumers say they know an organisation that does a good job at informing them how and why they are capturing personal data. In the US, that number is slightly higher at 25%. Payment service providers (PSPs) (68%), tech providers (65%), and retail banks (61%) occupy the top three spots in the UK among companies that do a good job of providing consumers with information about the usage of personal data. In the US, retail banks (71%) are first, followed by tech providers at 65%, and PSPs at 64%.

For digital natives, collecting data beyond personal information is better understood in comparison with older demographics. In both the UK and US, consumers between 18-24 years of age report higher awareness than other demographics when it comes to the knowledge of additional data being collected beyond their personal information.

Many consumers are aware that businesses are collecting data beyond their personal data to improve their online experience (e.g. device information, cookies, online behaviour, etc.)

Awareness of information collection beyond personal data

UK	18-24	25-39	40-54	55-69	Total
Personalised online customer experience	69%	64%	58%	52%	60%
Secure online customer experience	69%	66%	56%	52%	60%
Convenient customer experience	70%	60%	55%	49%	57%

US	18-24	25-39	40-54	55-69	Total
Personalised online customer experience	74%	71%	66%	57%	65%
Secure online customer experience	71%	70%	63%	56%	64%
Convenient customer experience	74%	69%	63%	56%	64%

With variations in consumer expectations based on demographics, preferences, and needs, businesses can no longer depend on a one-size-fits-all approach to online identification, where every customer passes through the same steps. In a market offering alternative options, if an onboarding process is cumbersome, consumers are likely to switch to a competitor offering a smoother experience. As a result, an abandoned account not only means lost revenue for the business but also translates into gained revenue for competitors.

Experian perspective

Leverage analytics and fraud orchestration for a 360° view of customers to mitigate fraud and offer a seamless customer experience: Businesses can have a clear view of customers and their behaviour across the network by leveraging the right tools at each step of the customer journey. This will help identify both good and bad patterns to mitigate fraud while offering a flawless customer experience to good customers.

The insights and data used to combat fraud can also enhance user experiences, providing clients with a deeper, more insightful view of their customers. Instead of battling the tension between fraud prevention and customer delight, the ultimate solution can simultaneously use the same capabilities to achieve both goals.

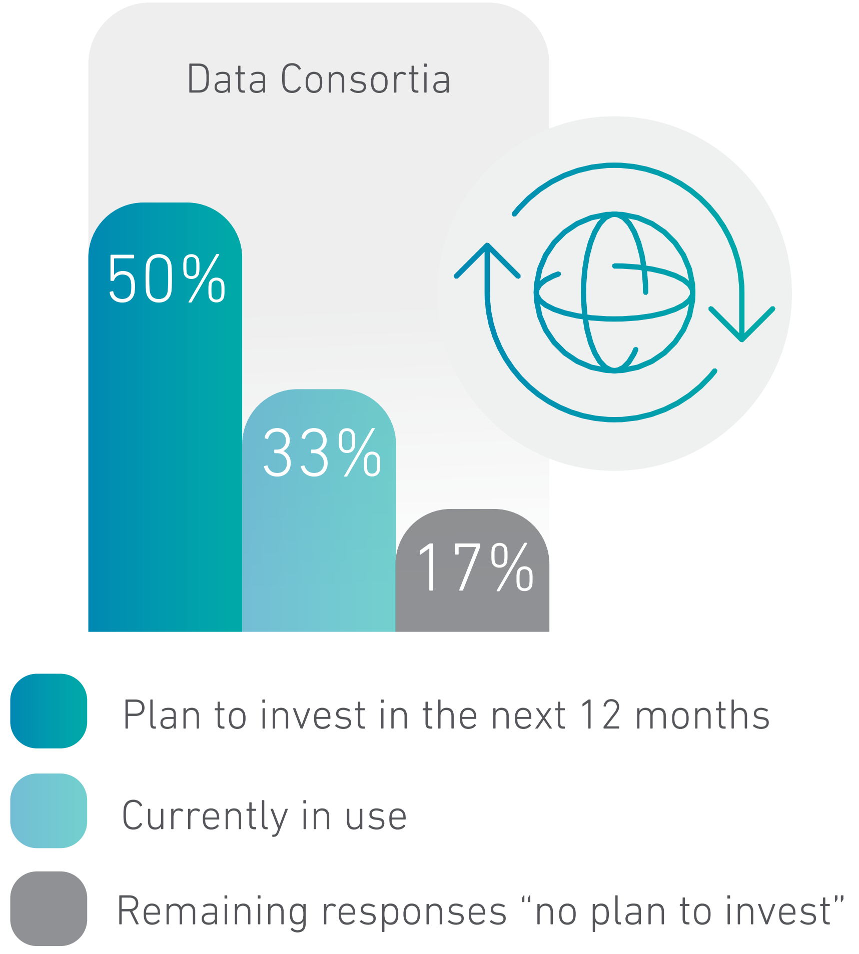
Removing unnecessary friction while keeping customers safe will improve the company's reputation and protect revenue streams.

Data sharing for successful fraud prevention

Fraud continues to affect businesses and consumers globally. Typically, businesses only have visibility of their own customer data, but data sharing enables them to gain insight and visibility of 'off-business' customers while benefiting from other observations across the network. This is why detecting fraud patterns through consortium data sharing across industries and borders is being recognised by businesses as an effective part of a fraud prevention strategy.

EMEA and APAC business respondents show high intent to invest in further data consortia tools for fraud prevention strategy, with 50% planning to invest in the next 12 months. A similar number of respondents (48%) agree that anonymised fraud data sharing between organisations will help to tackle the fraud problem.

Snapshot of current and future fraud prevention measures in EMEA & APAC

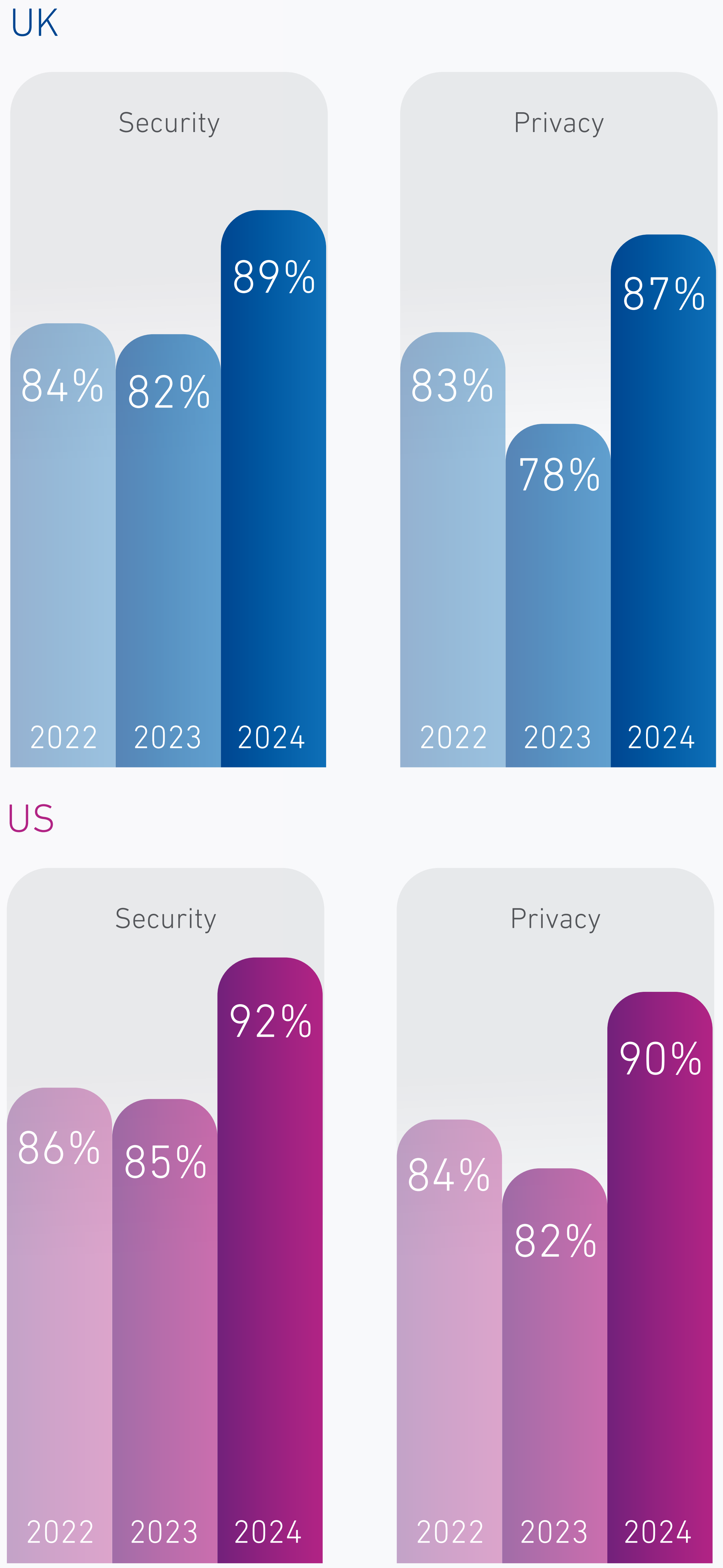


It is often the regulatory backdrop pushing for change when it comes to data sharing. In Brazil, the Central Bank and the National Monetary Council have enacted Resolution No.6, making it mandatory for financial services institutions to share data and information indicative of fraudulent activity. Similarly, in the UK, businesses are expected to support and encourage improved intelligence sharing to spot fraudulent transactions and stop them from happening.

Data sharing starts with data collection, so consumer willingness to share data to improve the online experience is critical. However, just 50% of US consumers report that they see the benefits of sharing their personal data with online businesses. For the UK, this number is slightly higher at 55%. Businesses should still strive to raise awareness about the positive outcomes surrounding this value exchange. With security cited as the most important dimension of the online experience for consumers in both the US and the UK, it's important to recognise that in the context of sharing data to prevent fraud – data sharing improves security rather than harms it.

Above all else, businesses must be willing to share their fraud outcome data with fraud prevention vendors to keep fraud performance optimised with minimal customer impact. A consumer sharing personal information with a business is just the starting point. To effectively combat fraud and ensure market safety, businesses must be open to collaboration.

Security and privacy are the most important dimensions for consumers when it comes to online experience



Making the connection: fraud and anti-money laundering (FRAML)

For a long time, businesses have been cautious about collaborating to detect economic crime, largely due to data protection and privacy laws. The UK's new Economic Crime and Corporate Transparency Act makes it easier for AML-regulated businesses to share customer data. It provides clear legal avenues for financial institutions to inform other relevant parties where they have refused or restricted a customer's access to a product due to suspicious behaviour.

Criminals often know a customer experience better than the business building it. However, if organisations can see fraudsters' infiltration on a holistic level through fraud signals in shared data, businesses can react more quickly to the threat. Access to data alone is insufficient—it must be connected, analysed, and constantly updated to drive better decision-making in fraud prevention. Good data-sharing schemes offer granular levels of control to all participating members in terms of shared data usage and contribution standards.

Experian perspective

As the Fraud and Anti-Money Laundering (FRAML) approach matures in places like the UK, shared AML and fraud risk data will become a core data asset for organisations and the key to maintaining up-to-date customer views. Moving towards a regulatory framework that allows for a single national fraud and economic crime database could help eradicate blind spots and facilitate data sharing. It is expected that more jurisdictions might consider this combined approach to remove operational silos and enhance criminal network countermeasures.

Data sharing is increasingly important: Fraudsters rarely operate in silos, and they likely reuse portions of the data they possess across multiple institutions. This opens the door for effective fraud mitigation through data sharing. Shared data will drive customer and risk decisions that benefit both the top and bottom line, protect customers, and close loopholes that criminals are currently using to perpetrate fraud, including the ability to identify money mules and their accounts.

Financial institutions should look for providers that can access, analyse, and share multiple sources of data to spot new fraud trends within their premises and stop risky transactions early. It is also important to work with partners, peers and vendors on safely sharing encrypted or hashed data, to ensure consumer privacy and data security.

The global rise of Authorised Push Payment (APP) fraud and the evolving regulatory environment

APP fraud works by tricking individuals into voluntarily transferring money under false pretences. Since these transactions typically use a real-time payment system, they are often irrevocable. According to the Global Anti-Scam Alliance (GASA), $1.026 trillion was lost to APP scams between August 2022 and August 2023. GenAI has accelerated occurrences of APP fraud by lowering the entry level for criminals seeking to commit this type of fraud.

Publicly accessible GenAI provides fraudsters with tools to generate more comprehensive and trustworthy phishing emails, engage with potential victims through chatbots, improve fake websites, and leverage deepfakes to gain the trust of prospective targets.

View APP Fraud Map

The most common fraud types encountered by US organisations in 2023 were:

- **32%** Account takeover
- **31%** Identity theft
- **31%** Fraudulent new account openings and applications
- **29%** APP or wire transfer payment fraud
- **29%** P2P payment scams
- **29%** Transaction payment fraud
- **29%** First party fraud

The most common fraud types encountered by UK organisations in 2023 were:

- **46%** APP fraud, money mules and scams
- **41%** Transaction payment fraud
- **34%** Identity theft
- **32%** Fraudulent account openings and applications
- **32%** Synthetic ID fraud

Legislative changes, such as the Financial Services Markets (FSM) Bill, are impacting financial institutions when it comes to APP fraud in the UK. The FSM Bill requires Payment Service Providers (PSPs), rather than consumers, to pay for losses related to APP fraud. Organisations have reacted to the new FSM Bill by implementing steps toward mandatory reimbursement. In the US, some initial steps could lead to regulatory changes, with congressional inquiries directed at the largest banks to seek out protective measures for consumers against fraud, looking to cross-industry solutions for better protection.

With consumers feeling the threat from APP fraud and regulatory pressures, US businesses recognise the need to respond. Improving how businesses detect APP fraud is the top fraud prevention priority for US business respondents, at 60%, and the third top priority in the UK, at 61%.

In addition, confidence in the ability to detect and protect against APP fraud is 81% in the US and 75% in the UK, indicating a deep understanding of the persistent threat of APP fraud globally, and thus its prioritisation. However, this dropped by 10 percentage points in the US between 2023 and 2024, indicating a possible change in sentiment.

Implementing measures to fight APP fraud is vital in helping financial institutions protect consumers and keep their reputations intact. With GenAI effectively boosting APP fraud, payment service providers should consider improving their defences against these types of fraud regardless of the regulatory advancements in their respective jurisdictions.

Two-thirds of UK businesses say they are primarily engaged in preventing first-party fraud. Increased economic pressure combined with the regulatory measures taken against APP fraud gives real account holders opportunities to try and report legitimate transactions as scams.

Experian perspective

Take steps to fight APP fraud regardless of regulatory pressure: While some markets are more advanced in regulatory measures than others, payment system providers can prevent APP fraud even if their respective jurisdictions are still in the early stages of defining the right set of measures.

APP fraud is a worldwide problem that has accelerated due to recent advancements in GenAI technology, and the progression of technologies related to faster payments, peer-to-peer payments, and alternative payment systems. By leveraging a variety of tools that include advanced data analytics capabilities, behavioural biometrics, transaction monitoring, anomaly detection, and fraud data sharing, in an appropriately layered approach, with smart orchestration directing the appropriate workflows, while actively educating consumers, businesses can better safeguard customers from APP fraud.

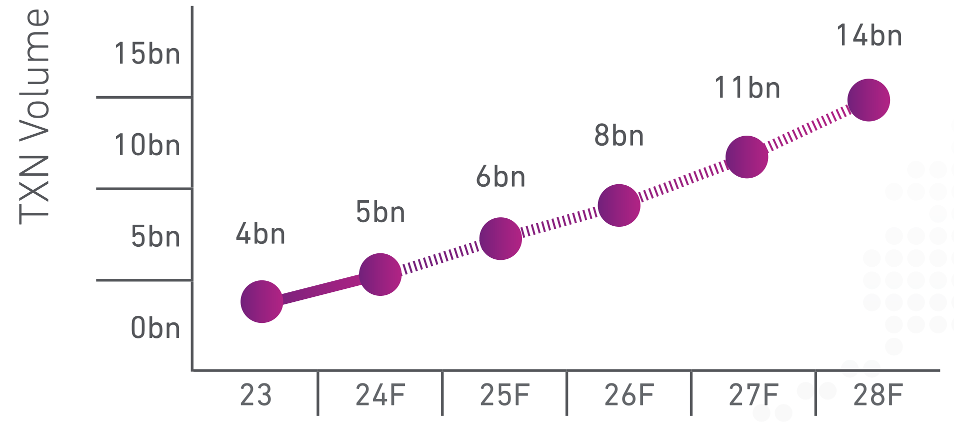
Tackling APP fraud allows businesses to maintain brand reputation, while preventing possible reimbursement costs, or loss of business due to consumers moving to competitors.

High-profile deepfake stories have entered the news more often over the past 18 months. Popular business and political figures or celebrities are regularly targeted to spread misinformation or trick people into fake investment opportunities. The biggest story to date involved a finance worker at a Hong Kong office of a multinational firm who was tricked into paying $25 million to fraudsters who used deepfake technology to pose as the company's Chief Financial Officer in a video conference call. Recent advancements in GenAI technology are paving the way for deepfakes to be deployed in real time. Although this is not a reality yet, it will allow fraudsters to perform such scams with ease.

As the growth of global real-times payments (RTP) continues, banks are coming under intense regulatory scrutiny related to liability and FRAML concerns

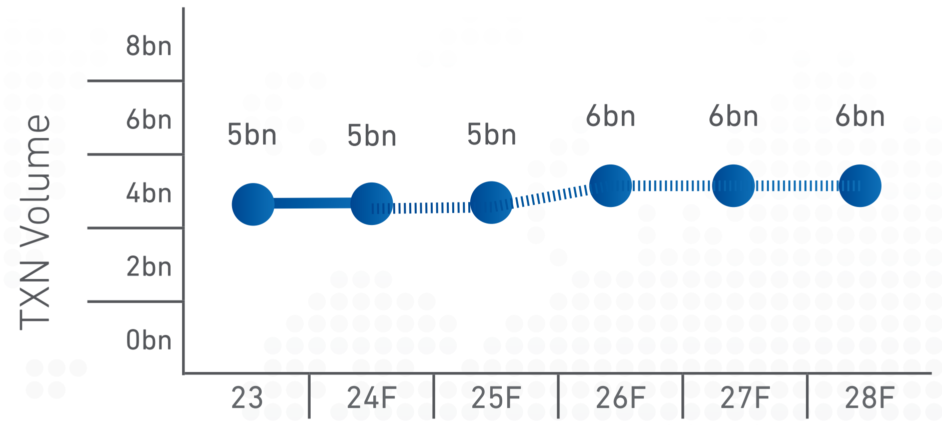
2023 global real-time payments reached c.266b transactions (42.2% YOY), valued c.$23T

US



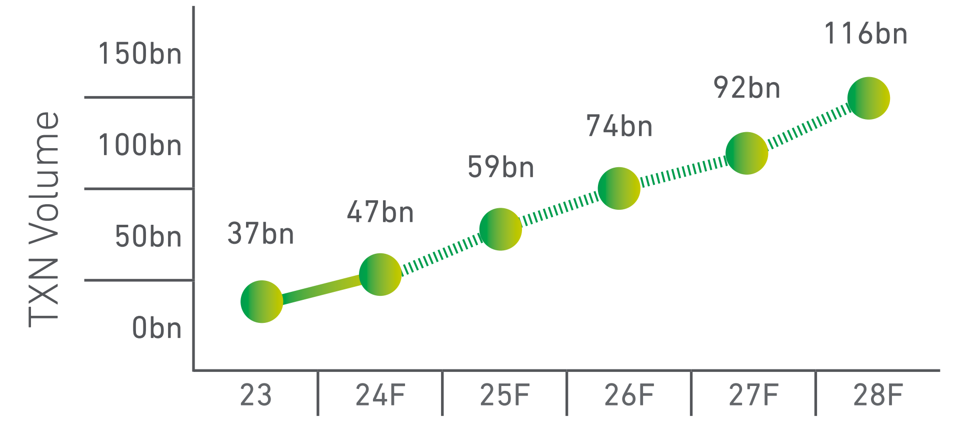
US real-time payments **are still nascent**, but growth is expected due to the launch of the **FedNow services**, at c. 32% 23-28F CAGR

UK



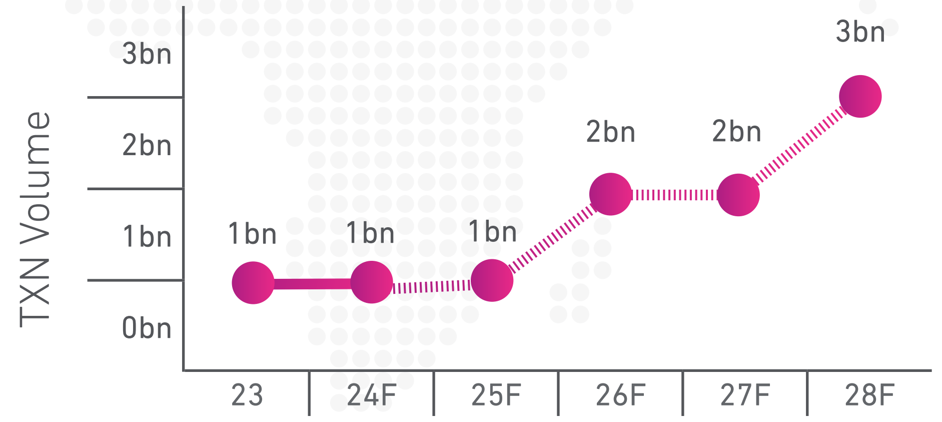
Despite plans to **overhaul real-time payments** in the UK via New Payments Architecture, repeated delays and revisions **left the status unclear**

Brazil



Driven by PIX, **Brazil makes up c.75% of LATAM's real-times payments market**, fostering an open ecosystem for FIs to support **PIX use cases**

Spain



Spain is still a **card-dominated market**, but strong growth is expected for instant payments in near-term due to **mobile-based Bizum service**

Key Takeaways

- Total global transactions are expected to reach **c.575b (17% CAGR) in 2028**.
- While the larger regions may be slower to adopt initially, over time, they will represent **an outsized portion** of the real-time transaction volumes.

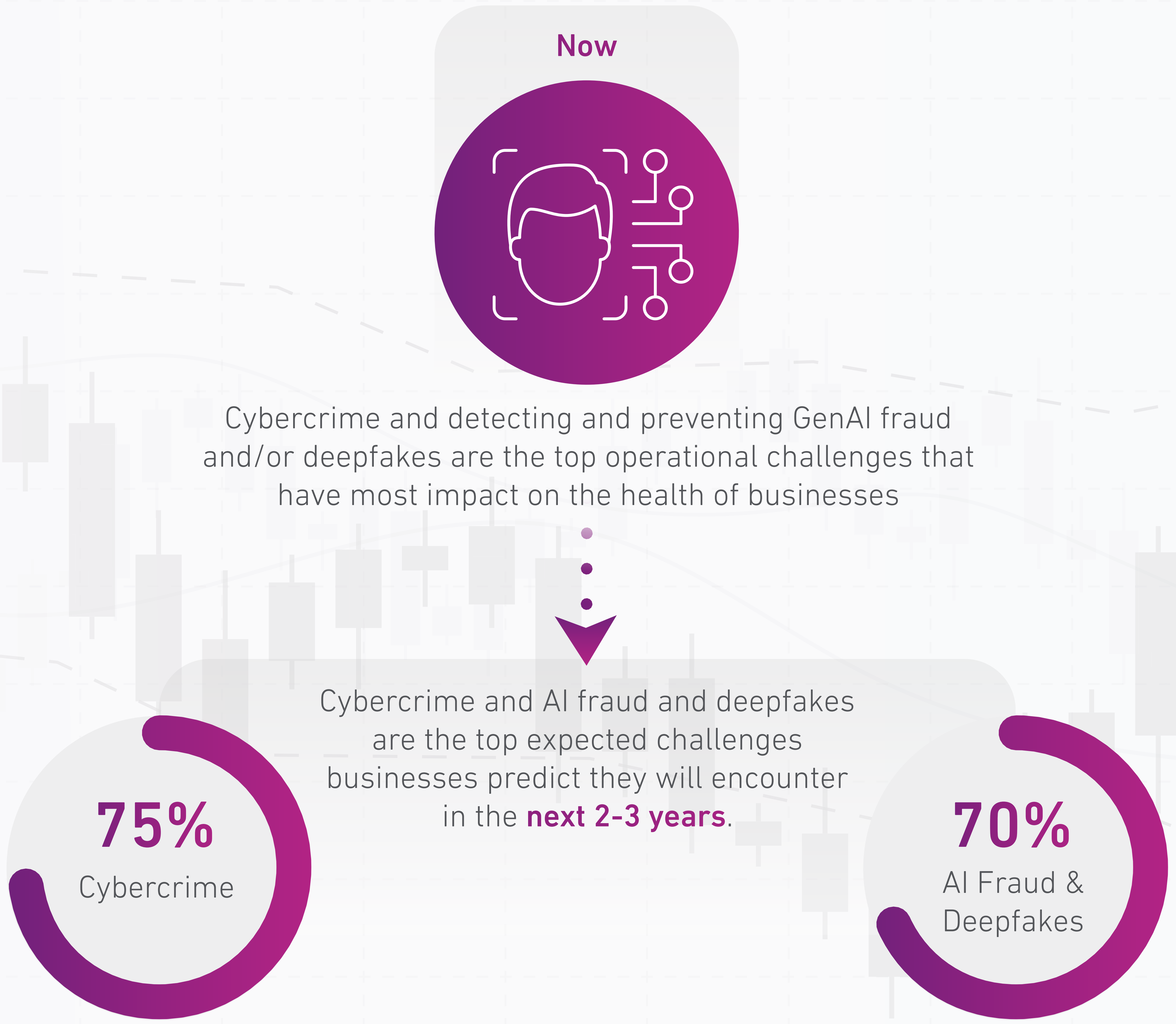
In Europe, the new **EU Instant Payments Regulation** is expected to drive instant payments volume across the 27 EU member states.

Source: ACI Worldwide

Uncovering synthetic identities in the age of Generative Artificial Intelligence (GenAI)

GenAI has also accelerated synthetic identity-related fraud by enabling the production of highly realistic fake images, documents, and social media profiles at scale for fraudsters to use across credit applications and new account openings. Synthetic identity fraud is reportedly costing businesses billions of dollars globally. Many organisations do not identify synthetic identity fraud correctly and classify it as a credit loss rather than a fraud loss, which makes accurate financial losses difficult to attribute. According to some estimates, synthetic identity fraud could account for up to 20% of loan and credit card charge-offs, meaning the annual charge-off losses in the US alone could be closer to $11 billion.

US: Operational challenges now and in the next 2-3 years that are putting the most stress on businesses and are having the largest impact on the health of the business



Now

Cybercrime and detecting and preventing GenAI fraud and/or deepfakes are the top operational challenges that have most impact on the health of businesses

Cybercrime and AI fraud and deepfakes are the top expected challenges businesses predict they will encounter in the **next 2-3 years**.

75% Cybercrime

70% AI Fraud & Deepfakes

Businesses focus on detecting and preventing synthetic fraud, but confidence is low

The widespread presence of leaked data has made it easier for fraudsters to create synthetic identities. Criminals combine legitimate and false data to avoid alerting the real owner, allowing them to smoothly pass through the onboarding stage and maintain their synthetic identity for longer, enabling higher-value attacks. With the help of GenAI tools, synthetic ID data is used to create accounts en masse, which may remain dormant until fraudsters need to move funds.

Our research indicates that 64% of businesses in EMEA and APAC experienced an increase in synthetic identity attacks from 2022 to 2023. In the UK, 62% of businesses plan to invest in synthetic identity fraud prevention and detection in 2024, while 56% of US businesses express an intention to do the same. Many companies in the financial services sector have relied solely on credit data to combat synthetic identity fraud. However, detecting these identities is challenging and requires many tools and resources. Specifically, digital signals such as device and behavioural intelligence have proven highly effective in this effort.

This sentiment is reflected in the recent data. Businesses see synthetic identity fraud as an operational challenge likely to have an impact. However, when asked about confidence in their ability to detect and prevent synthetic identity fraud, confidence was low, with the US ranking it 9th among other challenges and the UK 11th.

Businesses are already leveraging GenAI-related solutions

		UK	US
Solutions in use to detect and prevent fraud:	GenAI	25%	33%
Business emphasis/investment in identity authentication	GenAI	34% (4th place)	39% (4th place)

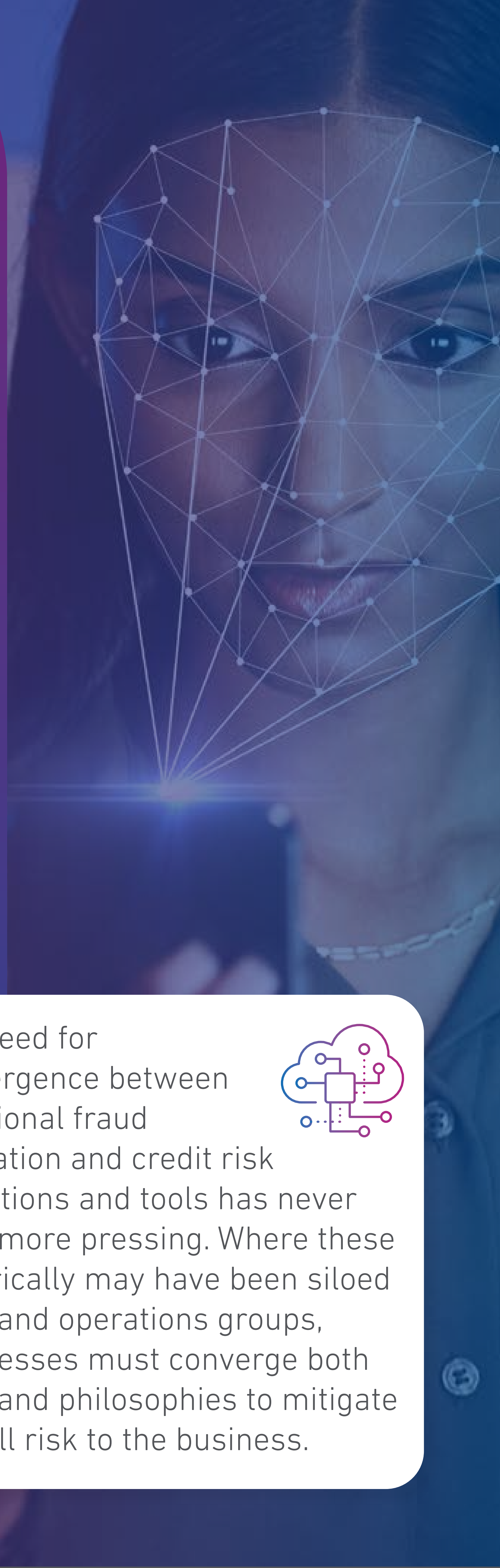
Experian perspective

One of the biggest **advantages of GenAI is that while it is being trained to create synthetic data, it can also be trained to spot associated anomalies** successfully.

Algorithms used to create deepfakes can also be trained to spot anomalies in audio, images, and video, such as inconsistencies in facial movements or features, inconsistencies in lighting or background, unnatural movements or flickering, and audio discrepancies. Businesses can also look at account opening channels from a variety of angles, deploying technology that monitors the behaviour behind newly created accounts. Alongside this, with access to alternative data sources businesses can ensure the discovery of linkages that are not contained in traditional credit data.

The use of passive signals from device and behavioural intelligence can provide a layer of insights that immediately detect when a fraudster is attempting to leverage synthetic identities. Fraudsters who have generated multiple identities will still need to use a device to interact with the webpage or app form. The power of detection becomes more about the method of the application than just the data in the application. Combining both data sets (the user-entered data and the device/behavioural/network data) provides an incredibly rich set of insights against which solutions can immediately identify discrepancies or anomalies across the full data payload.

The need for convergence between traditional fraud mitigation and credit risk operations and tools has never been more pressing. Where these historically may have been siloed tools and operations groups, businesses must converge both tools and philosophies to mitigate overall risk to the business.



The necessity of Artificial Intelligence (AI) and Machine Learning (ML) in fraud prevention

Moving away from the sole use of static rule-based analytics models in fraud risk strategy is almost universally understood by businesses as the only way to stay ahead of fraudsters in an era of rapidly evolving technology. With the abundance of data now available to businesses, the ability to ingest and manipulate data from multiple sources is paramount to achieving a frictionless customer experience and effective fraud prevention and detection.

To spot new and emerging fraud types, businesses are turning to AI and ML to respond to the unknown and get ahead of losses. ML models can identify both known and unknown trends in large data sets, so when a new fraud trend or type emerges, the ML model is able to identify it and immediately flag it to the security team for further investigation.

In EMEA and APAC three quarters (74%) of business respondents state that ML-based fraud detection is the most effective way to prevent fraud. However, only 14% of those using ML transactional fraud models reported updating them monthly or more frequently, with a third (32%) only updating their models annually. Having the right tools and staffing to update models regularly and keep on top of emerging trends is a challenge for businesses.

In the UK, investment in AI and ML has increased significantly. In 2022, 7% of businesses reported investing in AI and ML, but in 2024, that figure rose to 34%. Companies indicated that the primary reason for increasing investments in 2024 was to implement and enhance AI models aimed at improving customer decision-making (63%). This trend was mirrored in the US, where 62% of businesses stated that their higher investments in 2024 would likely focus on developing new AI models to enhance customer decisions.

For consumers, security is perceived as the most important online experience dimension in both the US (92%) and the UK (89%). At the same time, 92% of US consumers and 90% of UK consumers feel it is important for businesses they deal with online to accurately identify or recognise them on a repeated basis. ML allows large numbers of transactions or large data sets to 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.

Based on its ability to automate and enhance both fraud detection and online customer identification, ML has now become an essential technology for organisations that want to keep pace with consumers' growing online security expectations.

US

In the US, ML models receive high degree of confidence (**91%**) across businesses currently using them for customer authentication.

For fraud protection and detection, the level of confidence in ML models stands at **88%**

UK

Potential investment areas 2024

1st place: Implementing new analytics methods and building new AI models to improve other items that are not customer decisions (**16%**)

2nd place: Implementing new analytics methods and building new AI models to improve customer decisions (**15%**)

EMEA & APAC

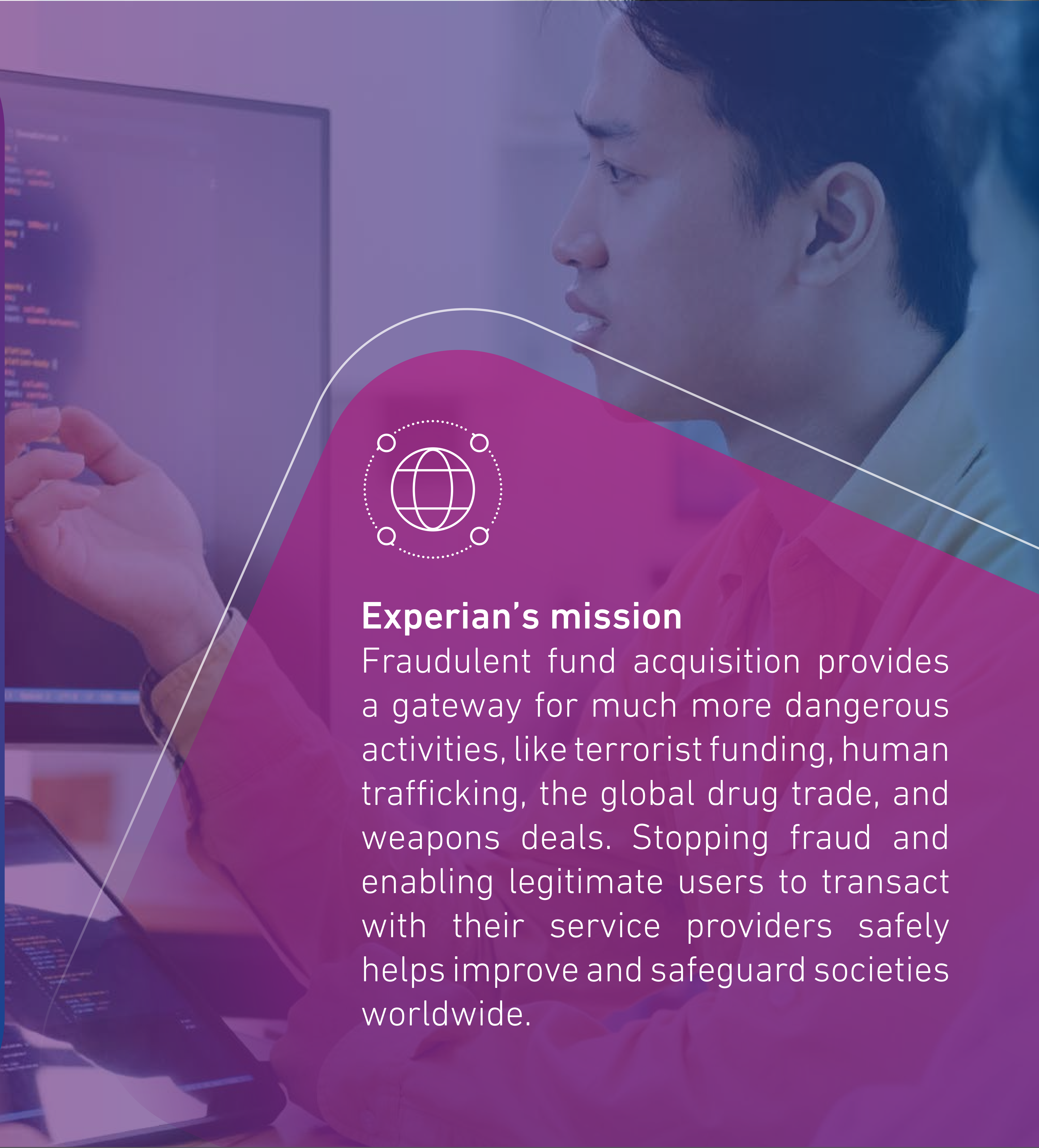
71% of firms believe that the future of fraud prevention will be driven by AI/ML based solutions

79% of businesses say that real-time monitoring with immediate fraud detection is the most important factor when considering ML-based fraud solutions

Experian perspective

AI and ML in fraud prevention can only be effective as part of a multilayered approach: AI and ML can streamline the discovery of existing and emerging fraud trends quickly and easily and prevent potentially fraudulent transactions from occurring before a business or its customers are compromised. ML can learn from previous fraud cases and analyse huge volumes of data to uncover anomalies and identify suspicious patterns that would otherwise be impossible for fraud investigators to detect. Although AI is considered a game-changer in fraud detection and prevention, it's not a silver bullet. Businesses must be able to monitor and analyse insights across the whole customer journey and tailor this to their use case using multiple interconnected tools. Only then can businesses understand the intent and context of every consumer before irregularities, anomalies, or fraudulent patterns translate into fraud losses.

Financial institutions should look for providers with fully integrated ML capabilities to reduce costs and take advantage of both pre-built or customisable models regardless of industry or size.



Experian's mission

Fraudulent fund acquisition provides a gateway for much more dangerous activities, like terrorist funding, human trafficking, the global drug trade, and weapons deals. Stopping fraud and enabling legitimate users to transact with their service providers safely helps improve and safeguard societies worldwide.

Five key takeaways

Deploying a multi-layered approach to combat evolving fraud

1. **Get a 360° view of customers to mitigate fraud and offer a seamless customer experience.** Leverage the right set of **fraud orchestration and analytics capabilities** at each step of the customer journey to help identify both good and bad patterns to mitigate fraud while offering a flawless customer experience to good customers

2. **Prioritise data sharing.** Access, analyse, and share multiple data sources to identify and prevent emerging fraud trends

3. **Take steps to fight APP fraud regardless of regulatory pressure.** Leverage a variety of tools that include advanced data analytics capabilities, behavioural biometrics, transaction monitoring and anomaly detection, and fraud data sharing, while actively educating consumers

4. **Uncover the use of synthetically generated content for fraud quickly and accurately.** Employ a layered approach that combines multiple tools, alongside data sharing, access to multiple interconnected data sources and analytics specifically tailored towards synthetic identity fraud

5. **Unlock the full potential of AI and ML for fraud prevention.** Fully integrate ML capabilities to reduce costs and leverage pre-built or customisable models for any industry or size. Combine these models with flexible rulesets to achieve optimal outcomes

Experian helped clients save

$15 Billion

in fraud losses globally in 2023

Research:

United States
Two major surveys conducted in the US in March of 2024: The first asked more than 2,000 U.S. consumers about their online interactions and expectations regarding security and customer experience. The second survey asked more than 200 businesses in the US about their strategies for effective fraud management, customer identification, and authentication, including investments related to security and customer experience.

Read Experian's 2024 US Identity & Fraud Report

United Kingdom
Two major surveys were conducted in the UK in March 2024: The first asked more than 2,000 UK consumers about their online interactions and expectations regarding security and customer experience. The second survey asked more than 200 businesses in the UK about fraud and AML management, customer identification and authentication, and investments related to security and customer experience.

Read Experian's UK Fraud and FinCrime Report 2024

Brazil
Two surveys were conducted in November 2023: The first consisted of 331 interviews with businesses in Brazil conducted via an online panel about investment focus, team, fraud management, and digital journey. The second survey involved 804 interviews with consumers in Brazil about their level of concern regarding fraud and identity theft.

Read more from Serasa Experian

EMEA & APAC
A survey was conducted in July 2023 in partnership with Forrester Consulting, asking 308 fraud leaders in the financial services, telco and ecommerce sectors across ten countries in the EMEA and APAC regions about the fraud environment.

Read Experian's EMEA & APAC 2023 Defeating Fraud Report

Contributors:

Mihail Blagoev, *Global Solution Strategy Analyst*, **Expert & co-author**
David Britton, *Vice President, Strategy, Global Identity and Fraud*, **Expert**
Rebecca McGrath, *Global Content Marketing Manager*, **Project lead & co-author**
Matthew Stennett, *Brand Design Manager*, **Design lead**
Paulina Yick, *Global Director of Product Marketing*
Christopher Wilson, *Senior Vice President, Portfolio Marketing*
Erin Haselkorn, *Head of Analyst Relations*
Michael Touchton, *Senior Manager of Analyst Relations*
Jean Sayers, *Content Lead, UK*
Jesse Hoggard, *Senior Marketing Director, Strategy & Innovation, North America*
Simon Pickering, *Content Lead, EMEA & APAC*
Raisa Kamaura, *Marketing Manager, Brazil*

experian.