



GLOBAL FRAUD SNAPSHOT 2025:

Opportunities and challenges in identity, fraud, and financial crime

Using the latest fraud and identity research from the UK, US, EMEA, APAC & Brazil, we examine the defining global trends shaping the fraud landscape in 2025.



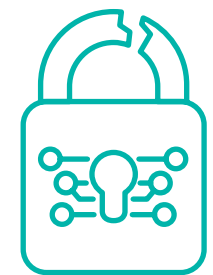
Rising consumer awareness, but trust remains fragile



57% of US consumers are concerned about conducting activities online, **12%** higher than in the UK



78% of US and **77%** of UK consumers are aware of online scams



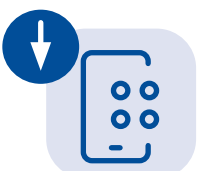
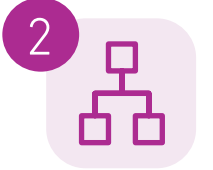
51% of consumers in Brazil report having been victims of fraud (up from 42% in 2024). **54%** of fraud victims lost money



86% of Brazilian consumers expect businesses to take security seriously



Consumers in both the **UK (87%)** and **US (83%)** expect businesses to act on fraud and identity concerns



UK and **US** consumers trust retail banks most when it comes to addressing concerns related to online activity and transactions, with peer-to-peer apps second. Social media sites/apps rank last in both regions



Despite rising awareness and expectations around online safety, consumer trust remains low — revealing a critical gap between digital engagement and confidence.

Business investment priorities for 2025

Top 3 global investment priorities across the UK, US, EMEA & APAC

US



Implementing new analytics methods and building new AI models to make improvements outside of customer decisions	64%
Improving detection and prevention of authorised push payment (APP) fraud	63%
Implementing new analytics methods and building new AI models to improve customer decisions	62%

UK



Improving detection and prevention of synthetic Identity fraud	55%
Implementing new analytics methods and building new AI models to improve customer decisions	52%
Implementing and improving AI models to improve customer decisions	52%

EMEA & APAC



Introducing machine learning (ML) based fraud models	46%
Lowering investigation costs	46%
Improving explainability of ML decisions	45%



Authorised Push Payment (APP) fraud has emerged as one of the most pressing global threats driving strategic investment and regulatory focus across financial markets worldwide.

- **63%** of **US** and **51%** of **UK** respondents say they want to invest in this area.
- In **EMEA** and **APAC**, **68%** of businesses say the fraud liability shift for APP fraud creates a stronger incentive for financial institutions to invest in improved security measures and fraud detection systems.

Global businesses are doubling down on AI adoption and fraud detection, with a focus on APP and synthetic identity fraud.



Operational stress & strategic gaps

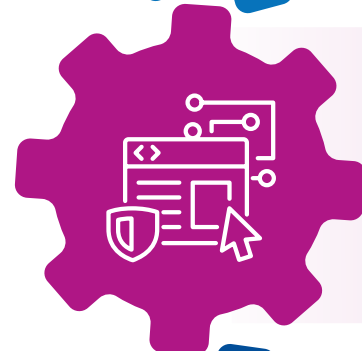
Fraud defence is fragmented, with limited cross-platform visibility and eroding consumer trust



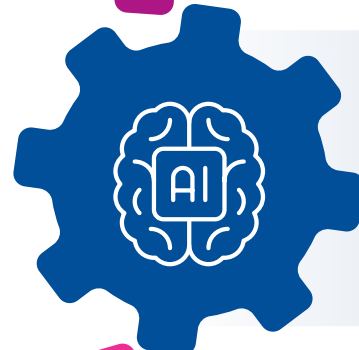
Identity theft is a top stressor in all markets



55% of respondents from **EMEA/APAC** expect their fraud losses to increase in the year ahead



76% of businesses in **EMEA/APAC** report that their organisation uses multiple fraud solutions from different vendors



GenAI fraud is increasingly seen as a critical threat vector in **all regions**



Only **27%** of **UK** and **32%** of **US** consumers can name a brand that does a good job of communicating how/why their personal data is being collected



Only **22%** of **US** consumers and **37%** of **UK** consumers express high confidence in businesses' ability to accurately identify them online



In Brazil, **69%** of consumers say it's extremely important or very important that companies can accurately identify users online

Businesses are overwhelmed by evolving fraud tactics—especially GenAI-driven threats—and are often forced to rely on siloed solutions from multiple vendors. This fragmented approach not only limits visibility across platforms but also contributes to declining consumer trust. Fewer than a third of consumers in the UK and US believe brands handle their data transparently or can accurately identify them online. Meanwhile, in markets like Brazil, consumers are placing increasing importance on businesses being able to identify users accurately, signaling rising expectations around identity assurance.

Consumer behaviour trends across the UK, US, & Brazil

Consumers continue to prioritise security over convenience, but friction during onboarding risks abandonment and weakens loyalty



Account creation remains high: **38%** of **UK** and **40%** of **US** consumers opened a new online account in the past 6 months



Frustration is real: **40% of US** consumers and nearly **30% of UK** consumers have considered abandoning a new account setup



Security over convenience: Across markets, over **80%** of consumers rank security and privacy above convenience or personalisation in digital experiences. In Brazil, **86%** prefer interacting with brands they perceive as secure and **62%** are willing to pay for safer experiences online



Despite increasing protection, only **18%** of **UK** and **16%** of **US** consumers feel they have full control over their personal data



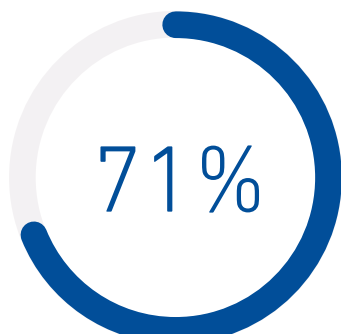
41% of respondents in Brazil would share data if it helped reduce fraud

Emerging opportunities

AI, biometrics, and fraud orchestration will be pivotal for reducing false positives and friction, yet many businesses lag in adoption due to complexity and cost barriers



AI is becoming a priority for businesses



of respondents in EMEA/APAC agree AI/ML-based fraud solutions will be critical to keep pace with growing fraud threats

Generative AI models are among the top investment priorities in customer authentication, cited by **41%** of **UK** respondents



In the US, **38%** of businesses are putting more emphasis on or investing in GenAI when it comes to identity authentication



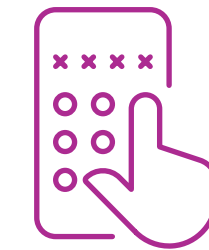
Biometrics rank highest in consumer confidence



Physical biometrics (facial/fingerprint) is the most widely used and trusted method in Brazil (**72%**)



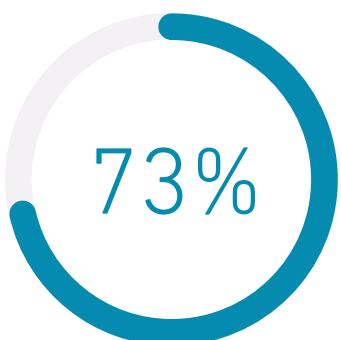
78% (UK) and **76%** (US) trust physical biometrics



66% (UK) and **72%** (US) trust behavioural biometrics (digital gestures/mouse movement)

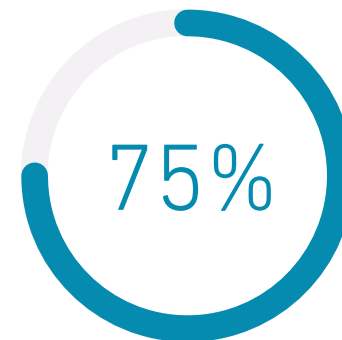


Fraud orchestration: Reducing friction, strengthening defense



of EMEA/APAC leaders say orchestration is key to reducing onboarding friction

of companies in Brazil say it is essential to have more than one layer of protection/solution against fraud



Fraud + Anti-money laundering (AML) integration

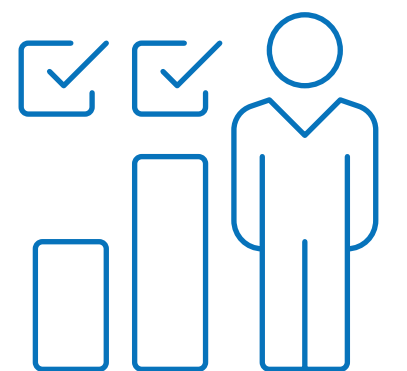


65% of EMEA/APAC and **60%** of UK firms are combining fraud and AML efforts



Consumers are willing to share data for stronger protection

65% of **US** and **76%** of **UK** would share more data if it led to improved security and privacy



About the research:

- 4,000 consumers across the United Kingdom and United States in March 2025
- 850 fraud decision makers across businesses in the United Kingdom and United States in March 2025, and EMEA & APAC in August 2024
- 877 interviews conducted in Brazil in November 2024

Where businesses must invest to stay ahead of fraud in 2025



A multi-layered approach to fraud prevention and detection across the whole customer lifecycle.

Combine traditional verification methods such as identity validation, document verification, and biometric checks, with more advanced services such as device intelligence, behavioural analytics, and behavioural biometrics to prevent complex fraud attacks, including synthetic identities and deepfake scams. Advanced analytics serves as an additional layer of intelligence—providing deeper visibility into fraud patterns, customer behaviour, and operational performance to help close the trust gap and reduce false positives without adding friction.



Smart fraud orchestration for adaptive protection. Apply intelligent fraud orchestration to dynamically respond to signals across disparate tools and vendors—creating a unified, real-time defense. Continuously test, refine, and update orchestration and decisioning logic to stay ahead of emerging threats while delivering the seamless experience genuine customers expect.



Integrating data and insights across credit, fraud, and AML. This convergence helps businesses build a more accurate picture of risk exposure—enabling them to detect fraud disguised as defaults or chargebacks and respond to the growing overlap between financial crime and credit risk.



Consumer education that helps raise awareness of emerging threats and available protections.

With identity theft and impersonation attacks making headlines, consumer awareness is more critical than ever in the fight against fraud. Businesses play a key role in this effort—not only by informing users about online safety and potential risks, but also by being transparent about how customer data is used to enhance security. Sharing this information helps build trust and underscores the importance of adopting new technologies that strengthen online experience and safeguard users.

How can Experian's multi-layered identity and fraud prevention approach help you deliver a seamless customer experience while mitigating complex fraud challenges?
[Click here to find out more](#)