# Building Trust in a World of Deception

Experian research conducted by Forrester Consulting

# Welcome to Experian's 2026 fraud report

**Over the past few years, we've seen the fraud threat expand considerably. It has become more organised and industrialised, with ever more powerful tools driving a surge in the scale and sophistication of attacks.**

Entire zones have become scam mega-factories that target innocent people across the globe. And there is an increasing threat from state-sanctioned criminal organisations' involvement in these coordinated attacks – leading some experts to suggest that we are in the midst of the golden age of fraud.

Confronting this challenge requires greater collaboration, as our individual efforts are much more effective when combined. Organisations that are part of Experian's network of fraud consortia often see a significant reduction in fraud losses by leaning on the collective intelligence shared across the group.

It has also become essential that businesses take advantage of the most advanced fraud prevention technology. AI has become a critical enabler of this defence, with both Machine Learning and Generative AI presenting new opportunities to better identify fraudsters, quickly adapt to changes, and more effectively manage fraud systems, thereby helping to protect businesses and their customers.

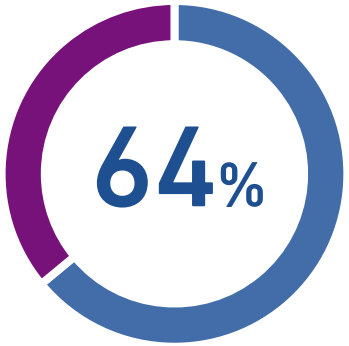
In this year's research, conducted in partnership with Forrester Consulting, we asked close to a thousand fraud decision-makers from nine countries for their views on the big trends impacting fraud prevention. I'm sure that their collective insights will help you refine your fraud strategy for the year ahead.

And whenever you're ready to start a conversation about our end-to-end fraud prevention platform, our global team of expert consultants is looking forward to talking to you.

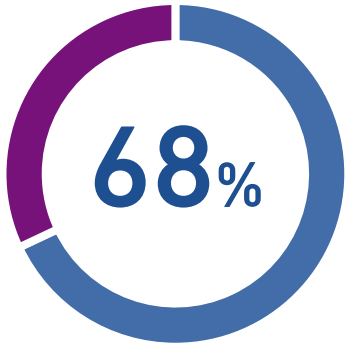
**SHAIL DEEP**
COO Experian EMEA & APAC

# Contents

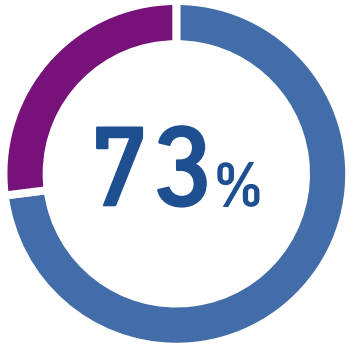
# Snapshot of key findings



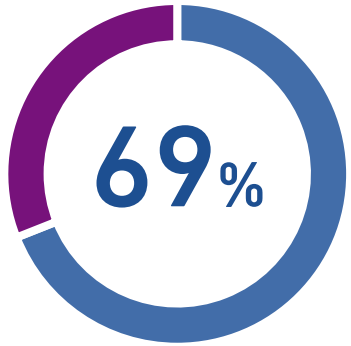

state that their fraud losses have increased year-on-year.



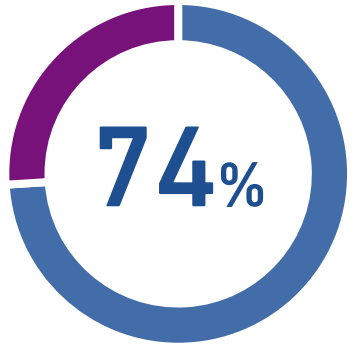

agree that their current technology stack is inadequate to counter a rapidly evolving fraud threat.




are interested in investing in passive fraud checks, like behaviour and device data, to minimise friction.




are planning to integrate fraud prevention and credit risk assessment into an overall risk management strategy.




agree that in the next three years, the majority of businesses will be part of a shared fraud intelligence group.

Base: 979 senior fraud decision-makers across EMEA & APAC
Source: Experian research conducted by Forrester Consulting, July 2025

PART ONE: Challenges and priorities

# Dispatch from the frontline

## Fraud has become faster and cheaper to execute than ever before. The dual threat of increasingly organised transnational cyber threats and GenAI-powered attacks has significantly increased the volume and complexity of attacks.

According to a recent study, Southeast Asia scam syndicates have become "the most powerful criminal network of the modern era", generating $50-70 billion per annum with a workforce of over 350,000. In addition, darkweb Fraud-as-a-Service vendors offer an increasing range of products to enable fraudsters with the latest tools and criminal intelligence.

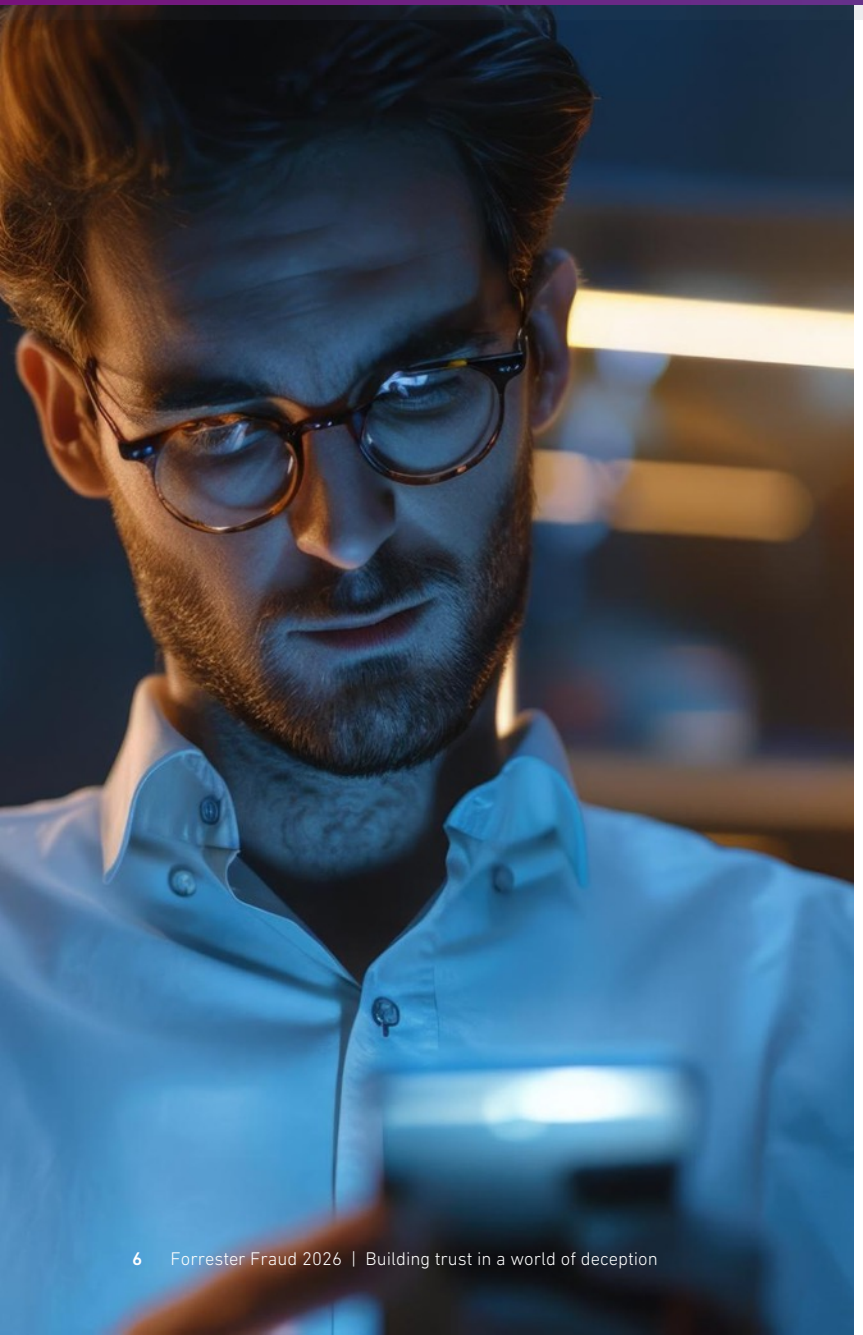
Our research shows that this threat is impacting businesses across the globe, with **more than two-thirds (67%) of respondents expecting more fraud attacks in 2026 than in the previous year, a 10% increase year-on-year.**

As a result of this onslaught, 64% of businesses are seeing their fraud losses increase from the previous year. The same percentage admits that their organisation is struggling to keep up with the rapidly evolving fraud threat. And the impact of this fraud tsunami goes beyond losses, as shown by the 67% who agree that fraud cases are damaging their organisation's reputation.

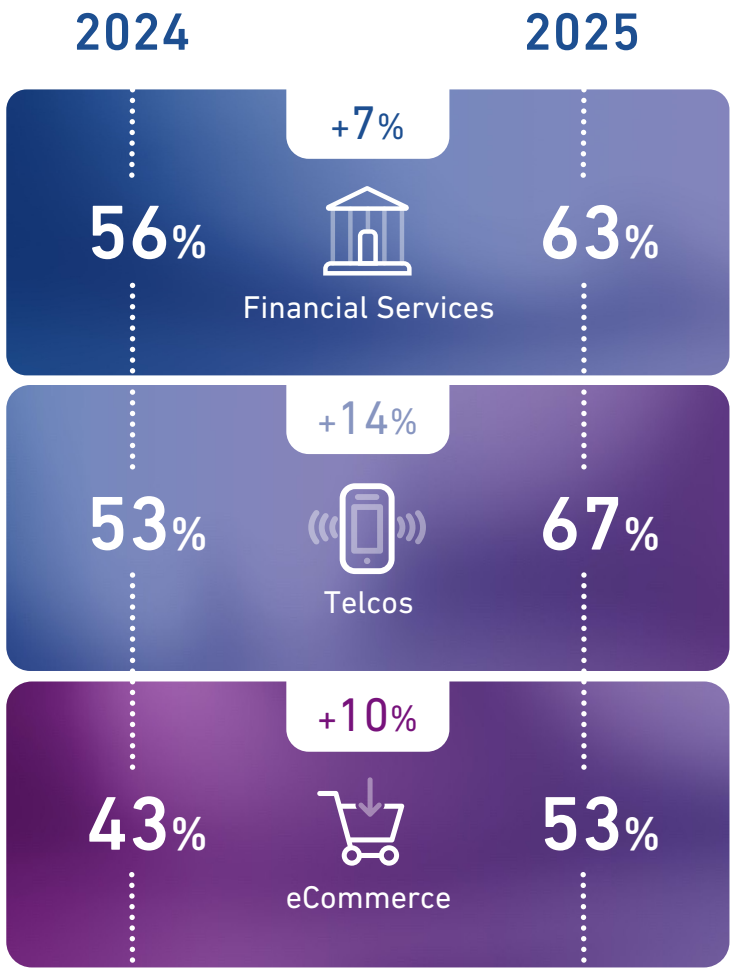
## Which types of fraud have increased the most?

Looking across the three industries we surveyed, Telcos have seen the biggest increase in overall fraud attacks, with over two-thirds (67%) reporting an increase. This is closely followed by Financial Services (63%) and just over half (53%) of eCommerce merchants.

**67%** expect more fraud attacks than last year



## Percentage of organisations reporting an increase in overall fraud attacks 2024 vs 2025




Base: 979 senior fraud decision-makers across EMEA & APAC
Source: Experian research conducted by Forrester Consulting, July 2025

Compared to the previous year, social engineering, loyalty/reward, and identity theft are the fastest-growing threats for FS and Telcos. It is no surprise to see social engineering rising, given what a powerful facilitation tool GenAI has become. The research also suggests that fraudsters are increasingly focusing on loyalty programs and rewards, perhaps due to perceptions that incentive schemes are generally less secure.

**Identity verification has become the most important security perimeter and the primary target of fraudsters**. As legitimate AI agents increasingly interact with websites along with bots and deepfakes, the ability to accurately authenticate and verify customer identity is vital.

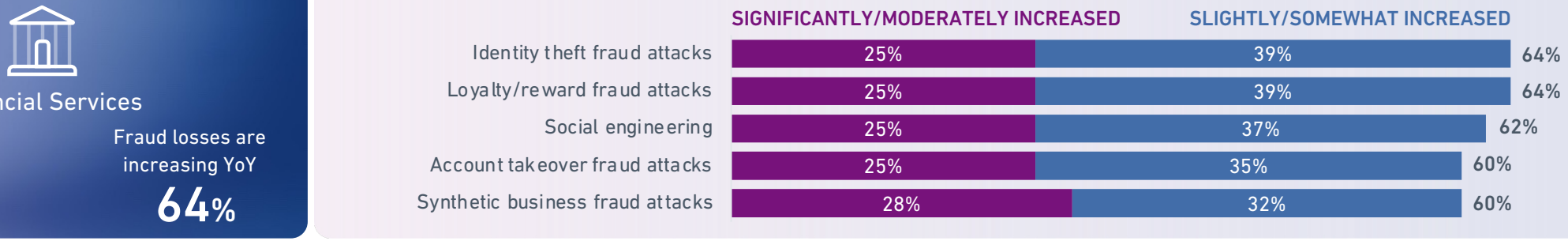
For eCommerce, friendly fraud and refund abuse have shown the biggest year-over-year increase. Synthetic identity fraud attacks have also increased, but not to the same extent.

## Year-on-year increase in fraud attack types by industry

### Financial Services

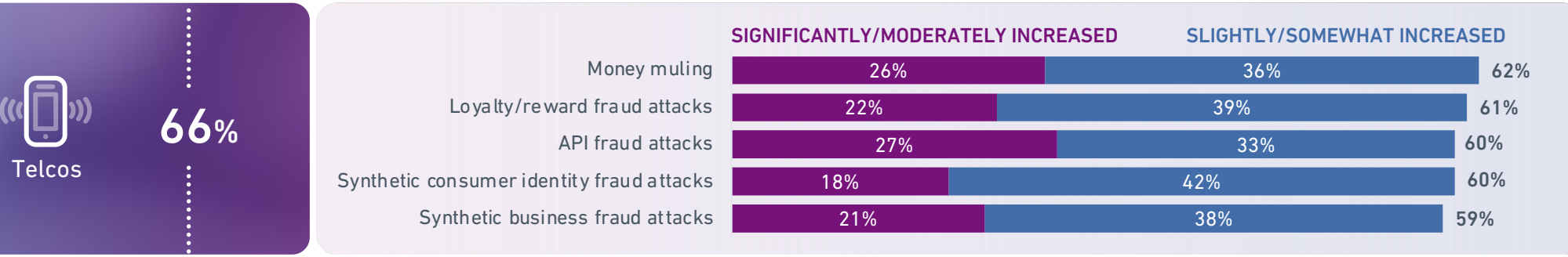
Increase in overall fraud attacks: **63%**

Fraud losses are increasing YoY: **64%**



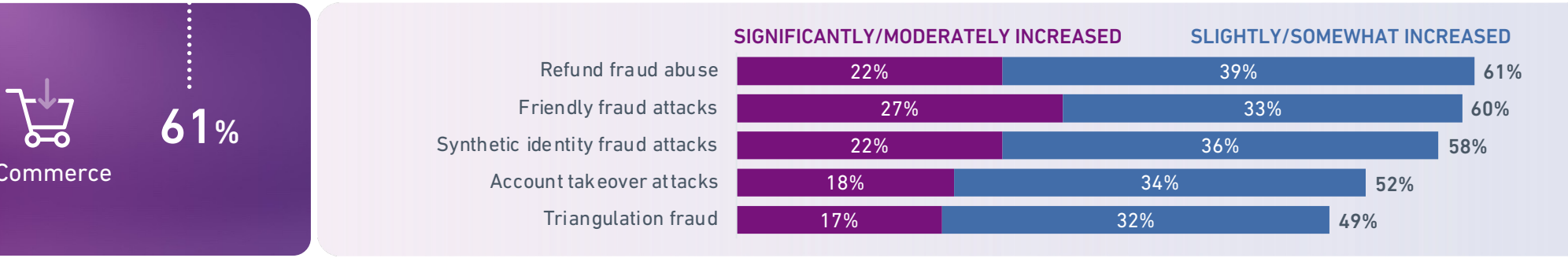

### Telcos

**67%** **66%**




### eCommerce

**53%** **61%**




Base: 979 senior fraud decision-makers across EMEA & APAC
Source: Experian research conducted by Forrester Consulting, July 2025

## Which types of fraud are the most challenging to detect and prevent?

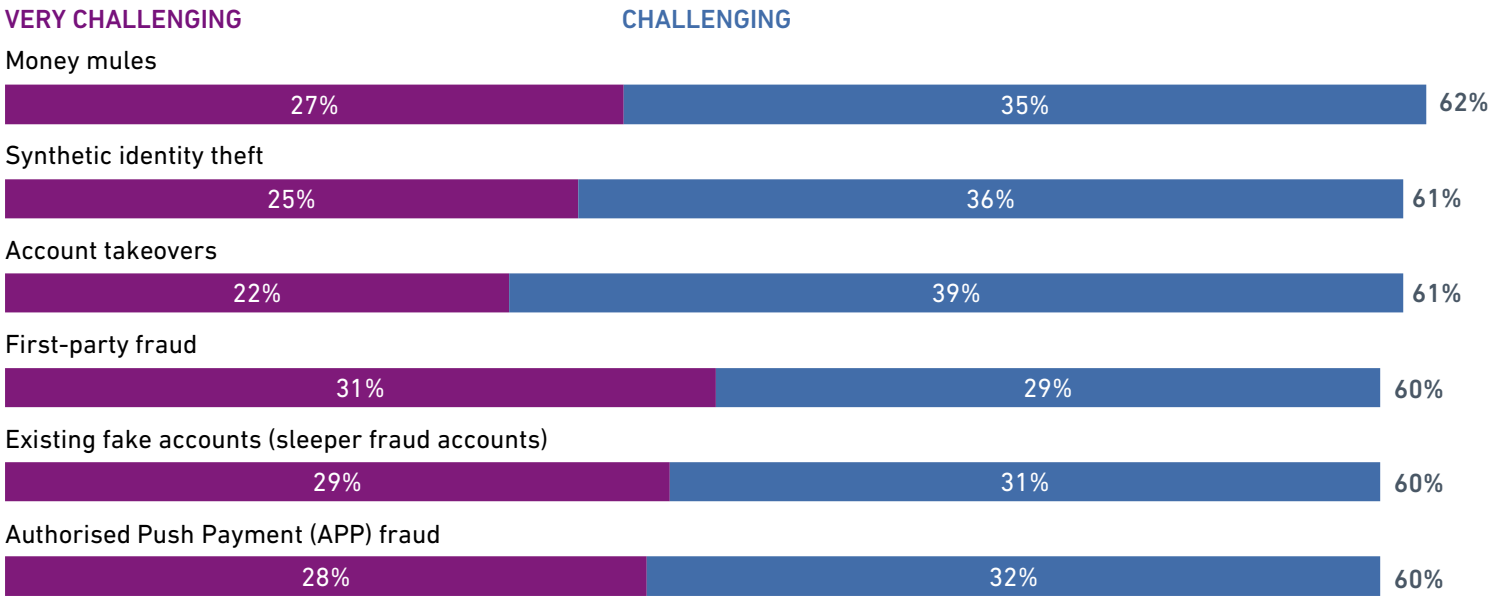
Our research shows that money mules are the most difficult type of fraud to counter, followed by synthetic identity theft and account takeover. This is where additional fraud signals have a crucial role to play, as they allow for continuous and passive monitoring of user data to identify patterns that can indicate these types of fraud.

Traditional authentication methods are now easily bypassed through GenAI-powered social engineering and dark web data. Fraud types that are difficult to identify can only be prevented through subtle device and behavioural signals that show when normal user behaviour has deviated.

Considering how few respondents are using advanced authentication tools, with only 42% currently using device data and 39% using behavioural biometrics, it is understandable why these types of fraud remain challenging to prevent.

Without these tools, many businesses will see fraud losses increase as fraudsters gain access to their systems with compromised credentials. Dark web monitoring has also become essential to keep track of what data is available and current fraud tactics.

### What are the most challenging types of fraud to detect and prevent?




Base: 979 senior fraud decision-makers across EMEA & APAC
Source: Experian research conducted by Forrester Consulting, July 2025

# Top fraud challenges

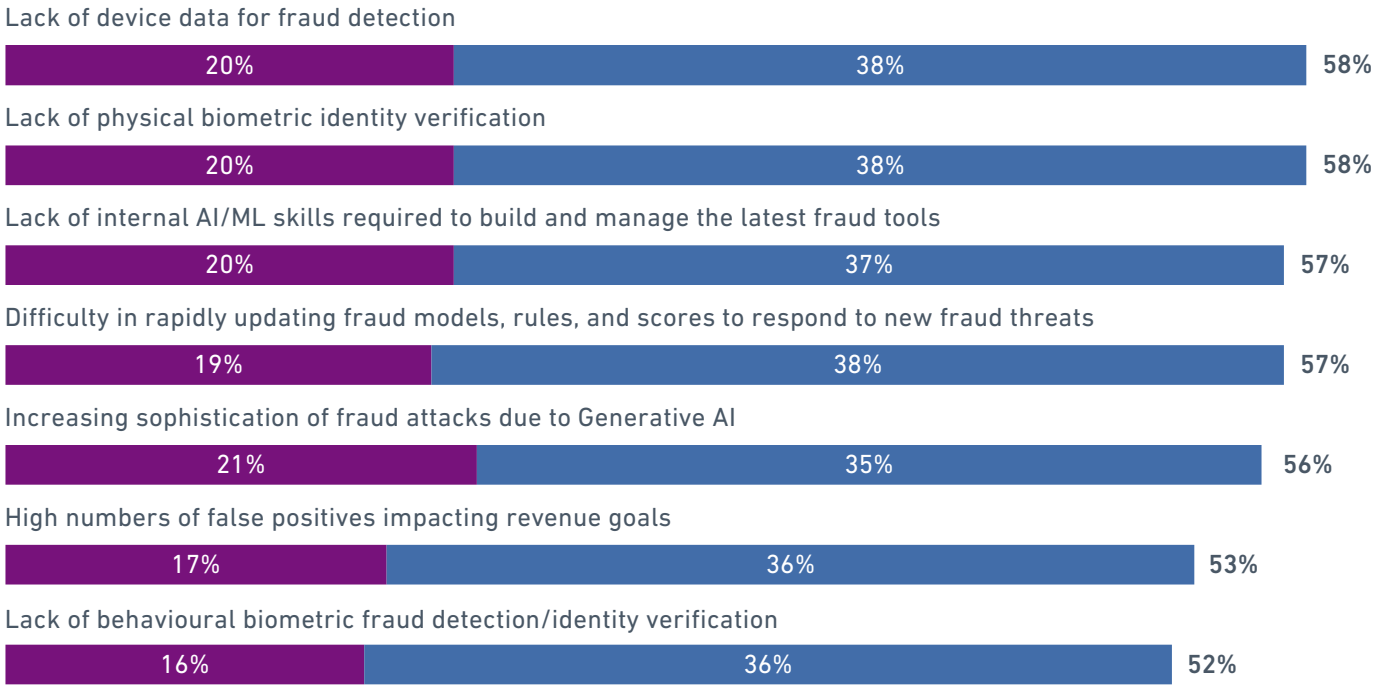
The top three issues limiting organisations' ability to detect and prevent fraud are all based on a lack of capability. Device data and physical biometrics are identified as the key missing capabilities and closely tied to these is the need for AI/ML expertise to transform these signals into accurate, reliable fraud decisions.

Our research suggests many businesses are caught in a capability gap, as their current fraud systems have become insufficient to control fraud, yet they do not have the capacity to introduce the advanced tools they need. This 'build vs buy' question is certainly not a new one, however, the rapid advances in the sophistication of fraud attacks have increased the pressure.

**Businesses need solutions now – not in a year or more, the time that it takes to develop a solution in-house.**
And balancing internal skills and capabilities against a growing fraud threat has become critical to future growth. It's interesting to note that close to three-quarters (71%) of respondents state that they are investing more in fraud technology than in human fraud analysts.

**68%** agree their current technology stack is inadequate to counter a rapidly evolving fraud threat

## Top challenges limiting the ability to detect and prevent fraud




Base: 979 senior fraud decision-makers across EMEA & APAC
Source: Experian research conducted by Forrester Consulting, July 2025

## The GenAI fraud juggernaut rolls on

If we look at the factors increasing the fraud threat, GenAI is the driving force that connects the vast amounts of data available on the darkweb with hundreds of thousands of captive fraudsters. Dark LLMs, such as WolfGPT and WormGPT, have enabled anyone with an internet connection to become skilled in a variety of fraud attacks.

As a result of this rapid shift in the quality of fake documents and deepfake images, 64% of respondents state that their existing KYC and identity verification checks are not equipped to detect GenAI-generated documents.

When real customer data is combined with synthetic images and documents, it becomes even more difficult to identify. And as ever more powerful tools are released to the public at lower costs, the problem is only going to get worse. Indeed, **60% agree that we have only seen the tip of the iceberg when it comes to AI-powered fraud.**

**66%** **of fraud experts agree that GenAI is the biggest challenge to fraud prevention ever**

An example of this rapid development is that video deepfakes now have heartbeats. Up until recently, this signal – skin tone variation based on heartbeat – was a reliable way to detect a deepfake. However, new advanced deepfakes can replicate this signal, which makes them even more difficult to detect.

There is no doubt that the advent of GenAI represents a watershed moment in fraud prevention. The boundary line between what is real and what is fake has been blurred, and the consequences are uncertain. 60% agreed that their fraud losses have significantly increased since GenAI. However, a similar percentage (58%) admit that they struggle to identify if GenAI has been involved in an attack and therefore find it difficult to quantify the impact.

## Should deepfakes be illegal?

61% of our respondents agree that deepfakes of all kinds should be made illegal for the benefit of society. Lawmakers across the globe are scrambling to formulate deepfake regulations, but the current vacuum of legal structure means the threat is almost entirely uncontrolled.

Denmark is one of the only countries that have responded with any kind of urgency to this issue by recently proposing changes to copyright law to ensure that everybody has the right to their own body, facial features and voice.

Italy has also taken decisive action by officially declaring the creation and distribution of harmful deepfakes a criminal offence under its new national AI law. This legislation, the first of its kind in the EU, introduces prison sentences for individuals who unlawfully produce or share AI-generated or manipulated content, including deepfakes. Penalties become even harsher if the technology is used to commit crimes such as fraud or identity theft.

This is a step in the right direction, but until further legal precedents are made, anyone can create a deepfake in seconds, so – should voice and video deepfakes be illegal?

# Priorities for the year ahead

In view of the increasing sophistication of fraud threats, it makes sense that the top priority for the year ahead is to strategically review current fraud solutions (70%). Systems that have worked for decades are fast becoming redundant and businesses are looking to include more fraud signals into their assessments.

This revaluation of fraud solutions ties in closely with the second and third priorities – **migrating fraud solutions to cloud (68%)** and **investing in new fraud tools (68%).**

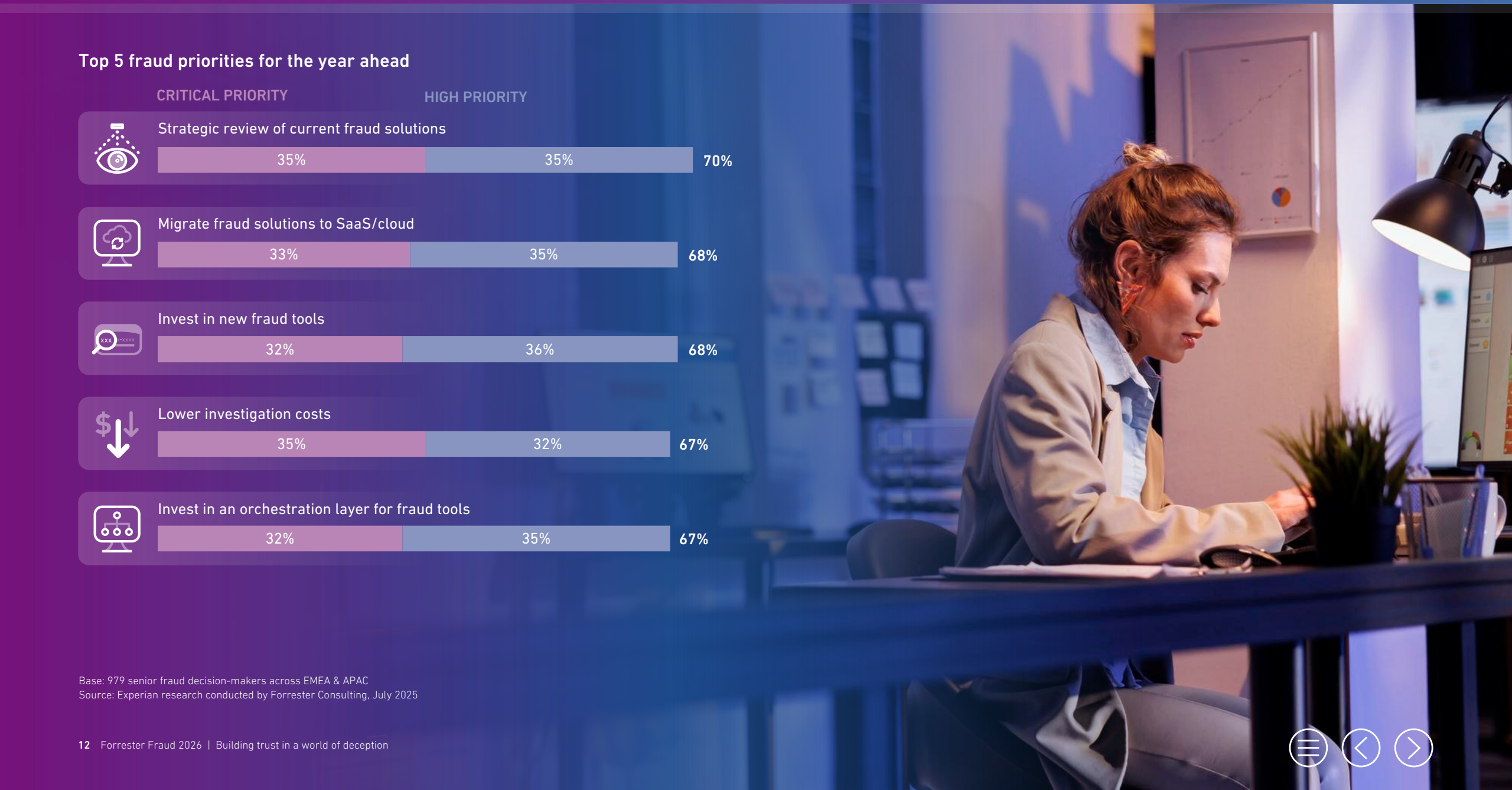
Looking ahead over the next 3-5 years, it is highly likely that the impact of GenAI on fraud is going to intensify. So strategically selecting which fraud capabilities to invest in is vital to avoid further losses.

Forward-looking businesses will build these capabilities onto a unified cloud-based platform rather than trying to stitch together different on-prem point solutions. And ultimately, the ability to combine fraud prevention and credit risk workflows will deliver the most powerful results. 69% of our respondents are planning to integrate fraud prevention and credit risk assessment into an overall risk management strategy in the near future.

**Lowering investigation costs** is also a top priority. While there are a variety of ways to achieve this, greater automation can play a significant role. Many fraud teams currently rely on manual reviews to resolve fraud threats, and more than a third (35%) state that it takes them a week or more to conduct a manual review. With the right fraud signals, a much larger proportion of decisions can be automated, which reduces investigation costs and allows fraud experts to resolve complex cases faster.

The final priority identified in the research **is investing in an orchestration layer for fraud tools (67%).** The same percentage of respondents agree that orchestrating multiple fraud solutions on a single platform is the future of fraud prevention. The reasons for this are clear, as orchestration improves customer experience and reduces costs by only calling fraud checks as required by the customer risk score.

## Top 5 fraud priorities for the year ahead




Base: 979 senior fraud decision-makers across EMEA & APAC
Source: Experian research conducted by Forrester Consulting, July 2025

PART TWO: Technology-driven solutions

# Why Machine Learning is essential to fight fraud

## The more data that is used to make an assessment, such as device and behavioural data, the more accurate the results.

However, making sense of this huge volume of data requires ML. Why – because only ML has the analytical muscle needed to extract insight from such vast datasets. Our research makes this clear, with **67% of ML users having seen a measurable improvement in the accuracy of their fraud detection since implementing ML**.

The second key benefit of ML is the ability to regularly retrain models on new data to stay up to date with changing fraud tactics. Rules-only systems struggle to adapt to new fraud types as new rules add complexity, increasing false positives and manual reviews. More than two-thirds (67%) of ML users agree that this ability to continuously retrain and update their ML models has helped them stay at pace with a rapidly evolving fraud threat. The same percentage has seen their false positive rate decrease since implementing ML.

ML

**70%**

**agree that ML has improved their ability to detect fraud that a rules-only system would have missed**

### How is ML impacting those businesses that have adopted it?

**67%**

Our false positive rate has decreased since implementing ML.

**68%**

ML has allowed us to reduce security friction for good customers by using passive fraud checks.

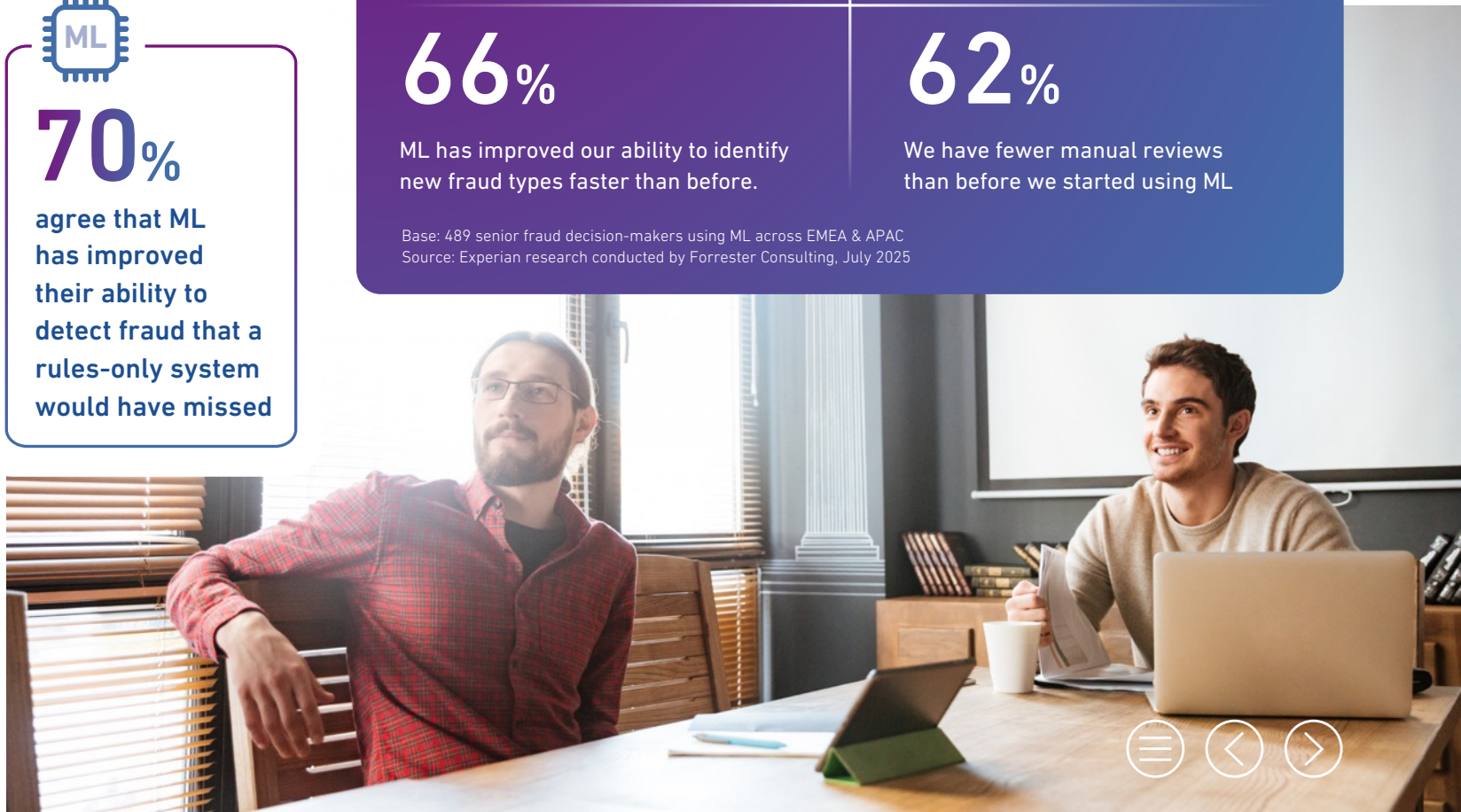
**66%**

ML has improved our ability to identify new fraud types faster than before.

**62%**

We have fewer manual reviews than before we started using ML

Base: 489 senior fraud decision-makers using ML across EMEA & APAC
Source: Experian research conducted by Forrester Consulting, July 2025



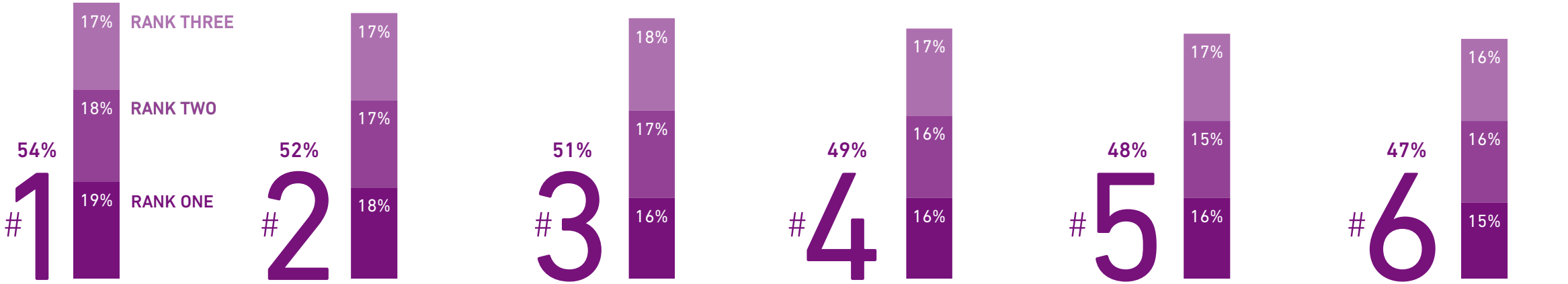
## What are the top benefits that ML provides?

Our research indicates that the biggest benefit of implementing ML is the ability to detect fraud threats in real time (54%). Only a third (33%) of organisations can currently detect fraud in real time, with a similar number (32%) taking a day or less, and 35% taking one week or longer.

Closely linked to faster identification is better customer experience (52%), which is ranked as the second biggest benefit. But customer experience is not just faster decisions, as reducing friction is also critical. Passive fraud checks that do not interrupt the customer journey are equally important.



### Identifying fraud in real time is the top benefit of ML



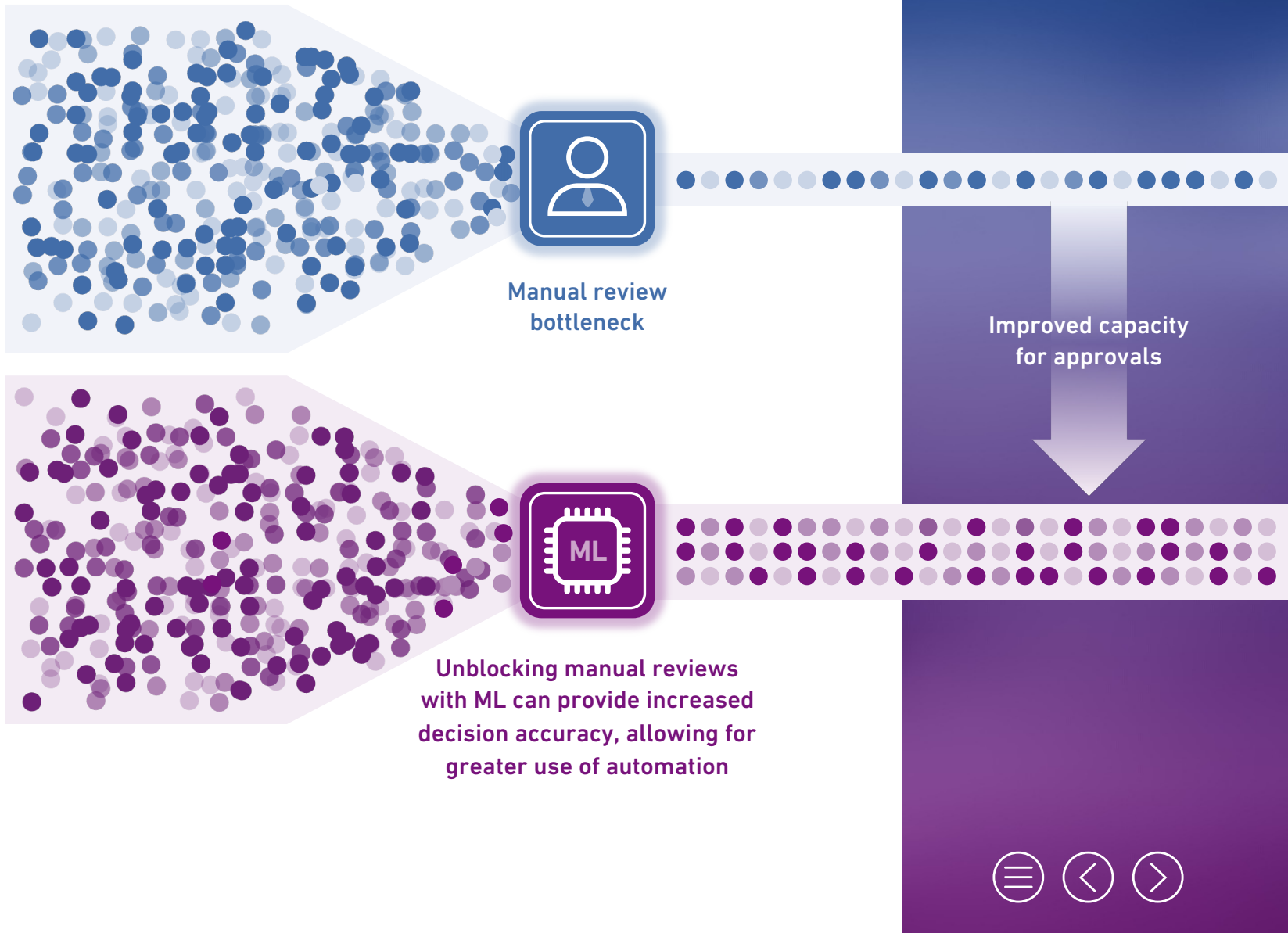

Base: 489 senior fraud decision-makers using ML across EMEA & APAC
Source: Experian research conducted by Forrester Consulting, July 2025

## ML can significantly reduce manual review bottlenecks

Nearly two-thirds (64%) of organisations rely on manual reviews to resolve fraud alerts, and this rises to 70% for eCommerce respondents. The impact of this bottleneck is that potentially good customers experience a slow and frustrating application or purchase journey, with a high likelihood that many will abandon it.

ML provides more accurate recommendations, which allows for more automation. Nearly three-quarters (71%) of those using ML agree that it allows them to better prioritise manual review cases, which has improved their fraud analysts' productivity.

**Monthly applications/purchases with and without ML**



## Why is ML not being adopted?

Comparing our latest ML credit risk research with this fraud research is revealing, some credit risk decision-makers do not understand the value of ML, and hence have not invested in it.

In comparison, the biggest reason holding back fraud decision-makers is a lack of quality data to train models (73% agree) – this suggests that many already recognise the value it can provide.

**The importance of having sufficient, high-quality training data cannot be overstated.** Accurate fraud prevention relies on having enough data from various sources, and with the advent of ML, the value of data has become even more important.

Training datasets must be large and correctly labelled for ML to provide accurate predictions. Pretrained off-the-shelf models can help overcome this challenge, as can the use of synthetic data to augment training datasets.

## Regulatory concerns about ML

Lawmakers across the globe are in various stages of legislating ML use in fraud detection to ensure transparency and fairness. Explainable ML enables declined customers to contest decisions, and full auditability helps to build trust in ML decisions for business users.

ML models can be fully explainable, with reasons provided for every decision, but uncertainty about what regulators are looking for and how to achieve this remain. 71% of our respondents would appreciate greater regulatory clarity on the use of ML in fraud prevention systems.

**More than two-thirds (67%) agree that a lack of regulatory clarity about acceptable ML fraud use cases is holding back their adoption of this technology.**

Internal capability

Regulations

Internal capability

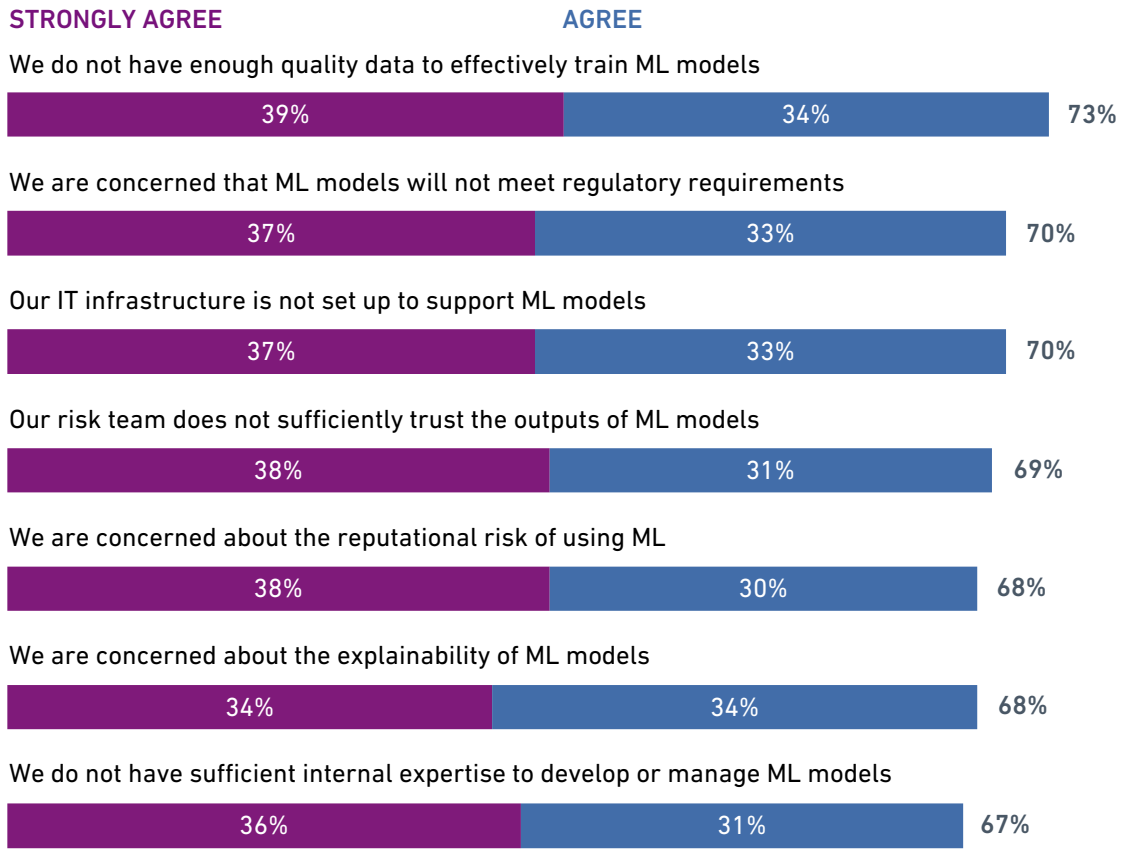
Trust

Reputation

Regulations

Internal capability

### Top reasons why ML has not been adopted




Base: 490 senior fraud decision-makers not using ML across EMEA & APAC
Source: Experian research conducted by Forrester Consulting, July 2025

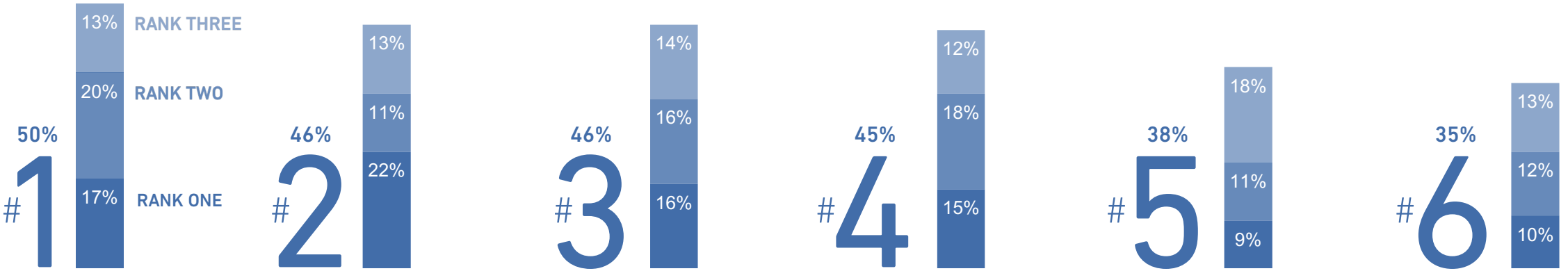
## What factors would encourage ML adoption for non-users?

Proven ROI from peers is the biggest factor that would encourage ML adoption. As with any new technology adoption, most businesses want to be the 'first to be second' so that they can learn from those who have gone before. Although this is a safer way to approach system changes, the current severe fraud threat demands a more proactive approach to adopting the most advanced fraud prevention technology.

Many businesses have already implemented ML with good results and positive ROI. For one Experian client that recently switched to an ML model, the timeframe to positive ROI was less than a month, as it identified a large syndicate attack shortly after going live.

Businesses interested in understanding the value of ML can arrange an offline Proof-of-Value (POV) assessment. This allows them to see the benefits that ML can provide based on agreed metrics without connecting their system to the model.

### Demonstrable ROI and clearer regulatory guidance would stimulate ML adoption




Base: 490 senior fraud decision-makers using ML across EMEA & APAC
Source: Experian research conducted by Forrester Consulting, July 2025

# GenAI assistants and digital identity wallets

## An exciting development in fraud management is GenAI assistants that are embedded in fraud prevention platforms. These tools can consolidate important data points, such as rules and their performance, fraud reasons and match durations (date/times).

They can also provide a case risk level, with appropriate justification and 'next step' instructions to complete an investigation. Additionally, they can streamline manual processes, improving both efficiency and decision-making accuracy.

Our research shows that 80% of respondents believe the biggest advantage of a GenAI assistant is to make their fraud prevention processes more accessible to less technical/non-coding employees.

### What could a GenAI fraud assistant do for your businesses?

**77%**

Believe the biggest advantage of a GenAI assistant is to reduce the time required to manage fraud cases.

**72%**

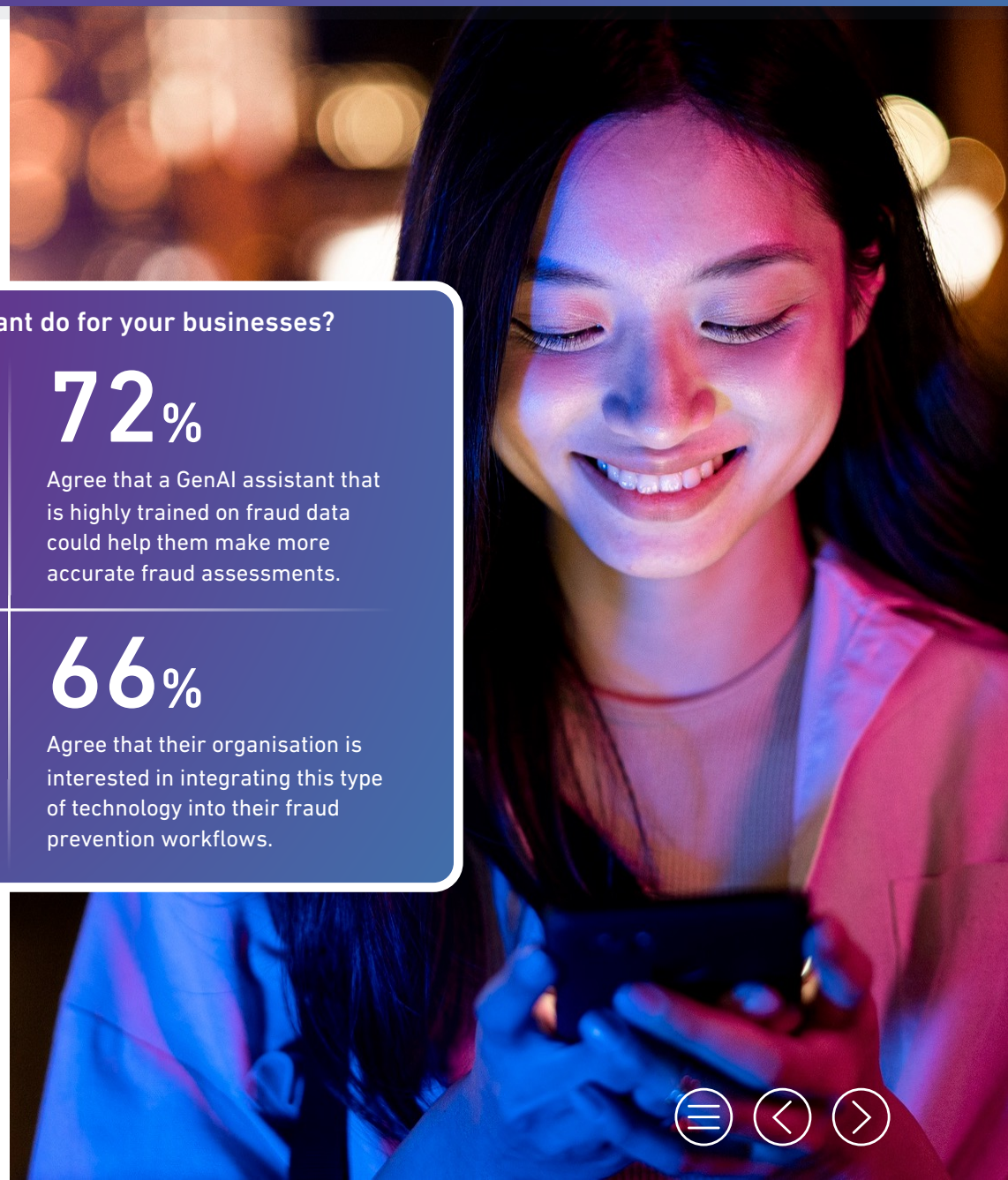
Agree that a GenAI assistant that is highly trained on fraud data could help them make more accurate fraud assessments.

**71%**

Believe that a GenAI-powered assistant could significantly reduce the time and effort required to manage new fraud cases.

**66%**

Agree that their organisation is interested in integrating this type of technology into their fraud prevention workflows.



Base: 979 senior fraud decision-makers across EMEA & APAC
Source: Experian research conducted by Forrester Consulting, July 2025

## The future of digital identities

The EU has recently outlined its plan for digital identity wallets to be recognised throughout the bloc and internationally, according to IDAS 2.0. In the next two years, all member states must offer digital identity wallets, and financial services and telco providers must accept them.

Digital ID initiatives are also being rolled out across Singapore, Malaysia, Australia and many other countries. India is leading the pack with its Aadhaar program, described as one of the most sophisticated digital ID systems globally and with over a billion registered users.

Nearly three-quarters of our respondents (74%) see digital identity wallets as a strategic opportunity to strengthen fraud prevention. A similar number (73%) are actively planning to integrate digital identity wallets into their customer journey.

Digital IDs have the potential to significantly reduce identity-related fraud, however, state and business education programs are essential to build trust in them and encourage adoption. The potential is significant, as seen by the 70% of respondents who agree that the introduction of digital identity wallets will fundamentally change how they onboard and authenticate their customers.

**74%**

**agree that widespread adoption of digital identity wallets could reduce reliance on traditional KYC and document verification**

# The growing shift to shared fraud intelligence

Collective fraud intelligence will undoubtedly have a significant role to play in the future of fraud prevention. **73% of respondents agree that the best way to counter the fraud threat is to collaborate and fight fraud together**.

However, this exchange of information needs to be facilitated by a trusted third party – three-quarters (75%) believe that building trust between different members of a fraud consortium is the key to their success.

Effective consortia require a central management hub, with secure API connections to each member. This allows sensitive data to be shared across the network while complying with data-sharing regulations. So that every application can be cross-checked against the collective intelligence pool without members sharing data directly between themselves.

**74%**

**agree that in the next three years, most businesses will be part of a shared fraud data group.**

For more information about how consortia work and the process of joining one, you can read Experian's consortia buyers guide:

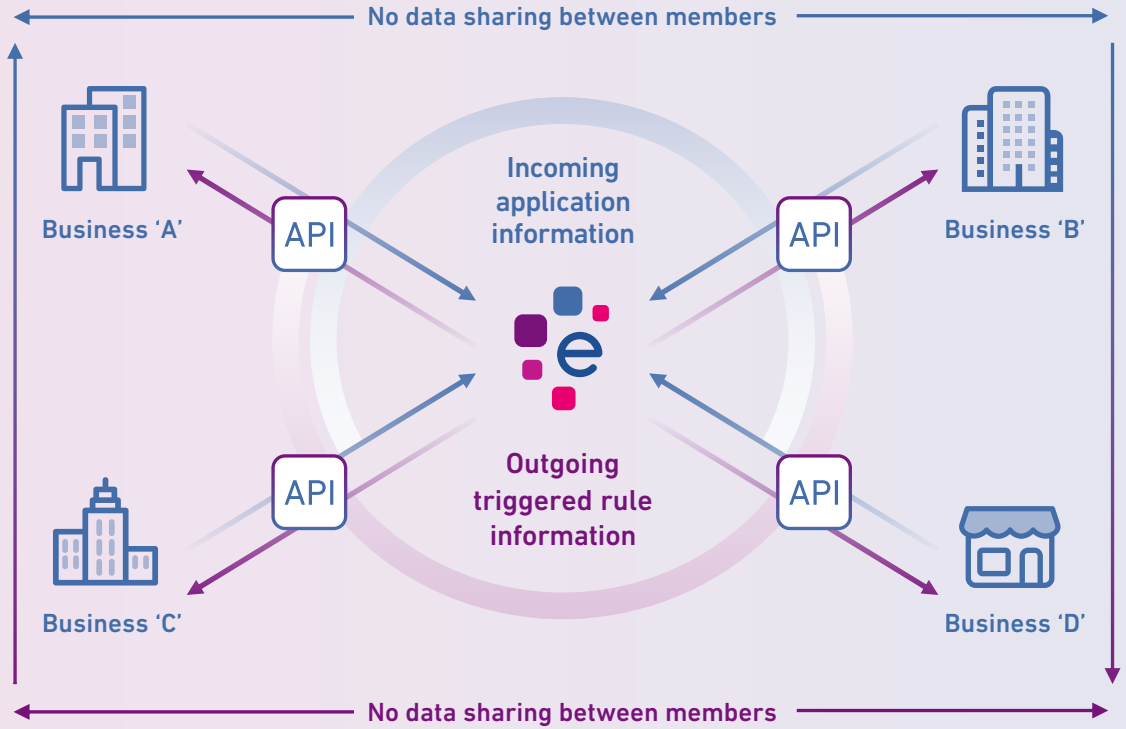
THE POWER OF SHARED INTELLIGENCE


## Data transfer process in a consortium

**1** Each business sends application/ purchase data to the central database via an individual secure API

**2** If the application data triggers an alert within the central hub, the rule that has been triggered is returned to the business

**3** No data is directly shared between business members



# Key takeaways

GenAI and deepfakes have changed the fraud threat forever. As these tools become more sophisticated, additional layers of fraud signals, such as device and behavioural data, have become essential to prevent a rapid increase in fraud losses.

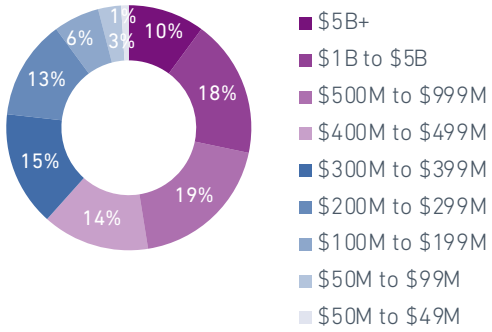
A strategic review of current fraud tools to identify capability gaps is the top priority for the year ahead, followed by migrating fraud solutions to cloud and investing in new ML-powered fraud tools.

The biggest advantage that ML provides is the ability to detect fraud in real-time, followed by improving customer experience through reduced friction onboarding/purchase journeys enabled by passive fraud signals.

Collective fraud intelligence sharing through consortia has a critical role to play in the future of fraud prevention, but this collaboration must be facilitated by a trusted third party to ensure regulatory compliance and trust between members.

# Firmographics and respondent demographics

## COMPANY REVENUE



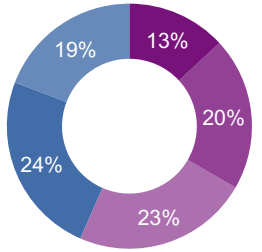

## GEOGRAPHY

N=~109 each country

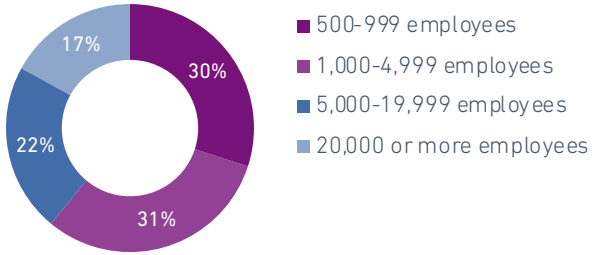
Denmark, Spain, Italy, Germany, South Africa, Norway

New Zealand, Australia, India

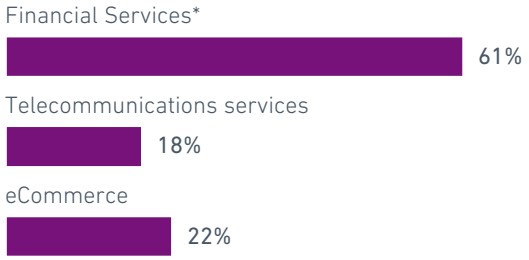
## RESPONDENT LEVEL




## COMPANY SIZE




## INDUSTRY




*Banking (38%), commercial finance/leasing (21%), automotive financing (25%), consumer lending (16%)

## DIRECT RESPONSIBILITY FOR DECISION-MAKING

# Glossary

### API FRAUD ATTACKS

Exploiting vulnerabilities in APIs to gain unauthorised access to data, denial of services attacks or manipulating the API in some other malicious way.

### AUTHORISED PUSH PAYMENT (APP) FRAUD

Fraudsters manipulate victims into willingly making payments to them through social engineering, such as pretending to be from a trusted financial institution.

### BEHAVIOURAL BIOMETRICS

Identifying and analysing data points associated with the subconscious way a specific user interacts with their device – without collecting PII data. These include mouse movements, keystrokes or touchscreen pressure and many hundreds of other behavioural attributes.

### BEHAVIOURAL ANALYTICS

Identifying bot attacks by comparing the way humans interact with devices versus the way bots interact with devices.

### BOT/CREDENTIAL STUFFING

Automated fraud attacks where lists of stolen credentials from one organisation are used to try and gain unauthorised access to an account at a different organisation.

### DEVICE PROFILING/FINGERPRINTING

Analysis of a set of software and hardware parameters associated with a specific device to provide a unique identifier and assess risk. These parameters include the operating system, network, browser, language, time zone, screen ratio and many more.

### DEVICE INTELLIGENCE

Device data combined with behavioural data is known collectively as device intelligence. It provides continuous and passive fraud detection signals.

### DEEPFAKES

Video, audio or images that have been convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said. In the fraud context, they can be used to fool KYC checks with a fake persona.

### FRAUD-AS-A-SERVICE (FAAS)

Fraud tools and services that are mostly sold on the darkweb on a pay-to-use basis.

### MONEY MULING

A person who helps launder criminal gains by receiving money into their account and then transferring it into another account on behalf of a fraudster. These middlemen are often recruited on social media and may be unaware that money muling is illegal.

### PHYSICAL BIOMETRICS

Unique physical characteristics that can be used to identify individual users. For example, liveness detection that uses facial recognition.

### SYNTHETIC IDENTITY

A combination of real and fake PII data is used to create a difficult-to-detect fabricated identity.

### SYNTHETIC BUSINESS

Like a synthetic consumer identity, these fake businesses use a combination of real and fake data to create the simulation of a legitimate business.

### TRIANGULATION FRAUD

An eCommerce scam where a fraudster creates a fake online store to collect payments from unsuspecting customers, then use stolen credit card information from a third party to purchase the same goods from a legitimate retailer and ships the product to the initial customer. The customer receives their order, the fraudster pockets the money, and the legitimate retailer is eventually hit with a chargeback from the stolen card's owner, resulting in financial loss and potential damage to their reputation.

# About Experian

## Experian is a global data and technology company, powering opportunities for people and businesses around the world.

We help to redefine lending practices, uncover and prevent fraud, simplify healthcare, deliver digital marketing solutions, and gain deeper insights into the automotive market, all using our unique combination of data, analytics and software. We also assist millions of people to realise their financial goals and help them to save time and money.

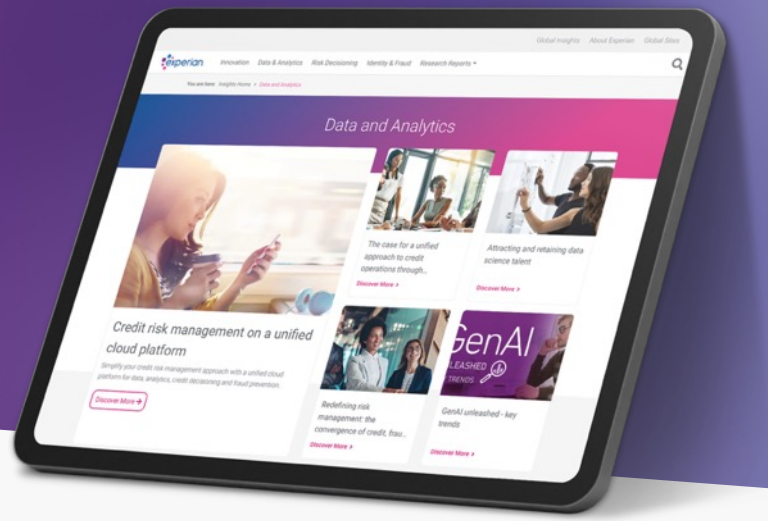
We operate across a range of markets, from financial services to healthcare, automotive, agrifinance, insurance, and many more industry segments.

We invest in talented people and new advanced technologies to unlock the power of data and to innovate. A FTSE 100 Index company listed on the London Stock Exchange (EXPN), we have a team of 25,200 people across 33 countries. Our corporate headquarters are in Dublin, Ireland.

**Learn more at experianplc.com**

Discover More →

Contact your local Experian consultant or visit experianacademy.com




Registered office address: The Sir John Peace Building, Experian Way, NG2 Business Park, Nottingham, NG80 1ZZ Telephone: 0844 481 9920 businessuk@experian.com experian.co.uk/business