DEFEATING FRAUD

AI as the guardian at the gates of digital business

experian.

WELCOME TO EXPERIAN'S
2023 FRAUD RESEARCH REPORT

Technology is a double-edged sword. The advent of Generative AI has changed the fraud landscape forever – by lowering the technical skills required by cybercriminals to launch attacks and putting previously secure identity verification techniques at risk. To counteract this formidable challenge demands an equally formidable solution – Artificial Intelligence (AI).

What sets this technology apart from legacy fraud prevention methods is its unparalleled ability to adapt and evolve. As the fraud threat mutates, only AI can analyse vast datasets in real time to identify patterns and proactively fortify defences. By harnessing the immeasurable power of data and Machine Learning (ML), AI stands as a guardian at the gates of digital businesses, ever vigilant against malevolent intent.

The old adage 'fight fire with fire' is highly pertinent in this situation – as the only way to fight back against the surge of AI-fuelled fraud is with AI-powered fraud prevention tools. These need to be implemented in a multilayered approach that continuously scans each user session for signs of fraud.

For a deeper understanding of the fraud environment, we commissioned Forrester Consulting to survey 308 fraud leaders in the Financial Services, Telco and eCommerce sectors across ten countries in the EMEA and APAC regions: Australia, Denmark, Germany, India, Italy, New Zealand, the Netherlands, South Africa, Spain and Turkey.

In this report, we reveal the key findings and discuss why AI is becoming essential to safeguard businesses from fraud. Experian has always been committed to making the digital world a safer place through innovative fraud prevention solutions and expert consultancy. I hope you find the insights valuable, and I encourage you to reach out to us to discuss how we can help you along your fraud prevention journey.

FRANCESCO NAZZARRI
CCO Experian EMEA & APAC

SNAPSHOT OF KEY FINDINGS

73%

have seen an increase in fraud losses over the past year.

70%

find that false positives cost their businesses more than fraud losses.

50%

expect their fraud losses to increase in the next 12 months.

77%

agree that biometrics are the most effective way to verify customer identity.

73%

agree that device intelligence is a must-have component of fraud prevention.

72%

agree that the future of fraud prevention will be driven by AI/ML-based solutions.

Base: *308 EMEA & APAC fraud decision makers at Financial Services, Telco and eCommerce firms*
Source: *Experian research conducted by Forrester Consulting, July 2023*

ONE

ON THE FRONTLINE OF FRAUD: AN OVERVIEW

The relationship between challenging economic conditions and increased fraud losses is well documented, with a causal relationship between the two. Although 2023 has seen inflation and energy prices easing from last year's highs, recovery from the current economic slowdown is predicted to be gradual. As a result, the fraud risk is likely to remain elevated for the foreseeable future.

Nearly three quarters (73%) of our respondents have seen an increase in fraud losses over the past year. Financial Services took the biggest hit, with 78% seeing an increase in losses. These shocking figures illustrate the severity of the fraud threat for businesses and suggest that the impact of economic uncertainty is being compounded by several other factors.

The first of these is the ongoing surge in digital adoption. This trend was greatly accelerated by the pandemic and as the digital marketplace grows, the potential for fraud grows with it. The second is the increase in data breaches, which directly contribute to fraud as an ever-increasing volume of private data becomes available via the dark web. Perhaps the most significant factor is the public availability of Generative AI (GenAI).

While we are only just starting to understand the impact of this powerful technology the implications for fraud are profound. The recent arrival of malicious large language models, such as **FraudGPT**, is driving a new wave of social engineering and phishing attacks. Moreover, these models can now be used to write adversarial code and create fraud automation tools, thus reducing the technical barriers to conducting fraud. Of particular concern is the ability of GenAI to write polymorphic code that continually creates different versions of itself while retaining its original function.

GenAI is likely to also impact the ability of businesses to effectively conduct customer due diligence (CDD) and know-your-customer (KYC) checks, as it allows fraudsters to create high-quality forgeries of documents such as utility bills, proof-of-residence and bank statements. These can be combined with **highly realistic fake images** and stolen ID data from the dark web to create convincing synthetic identities.

The breakneck pace of change exacerbates this situation as even previously secure identity verification techniques, such as voice recognition, are now under threat. Adapting to these challenges is difficult, with 71% of our respondents struggling to keep up with the rapidly evolving fraud threat. Another telling indication of the rate of change is that 50% expect their organisation's fraud losses to increase over the coming year.

78% OF FINANCIAL SERVICES

have seen an increase in fraud losses over the past year.

71% OF OUR RESPONDENTS

are struggling to keep up with the rapidly evolving fraud threat.

On the frontline of fraud: an overview

Year-on-year fraud attacks are up

Year-on-year the volume of fraud attacks has gone up in almost every category. Synthetic identity attacks have shown the largest growth with 64% of Financial Services and Telcos reporting an increase. This is closely followed by identity theft attacks and account takeover attacks – with 60% of respondents reporting an increase in these categories.

Synthetic identities are becoming easier to create due to the prevalence of leaked data. Fraudsters can strategically use legitimate data, combined with false data, to avoid alerting the real owner that their identity has been compromised. They are often able to move through the onboarding stage and cultivate their synthetic identity for a longer period in order to conduct higher-value attacks.

In the past, phishing attacks were often clumsy and easily identifiable due to poor construction. However, with the arrival of malicious GenAI tools, the sophistication and elegance of phishing and social engineering attacks have improved considerably. This will inevitably result in an increasing number of unsuspecting victims handing over their details – with a corresponding increase in account takeover.

The rise in API attacks (57%) is also cause for concern, as this can result in huge volumes of private information being lost, as well as service disruptions. APIs are particularly susceptible to automated or bot attacks and businesses need specialised API fraud detection algorithms – that investigate multiple signals – to protect them.

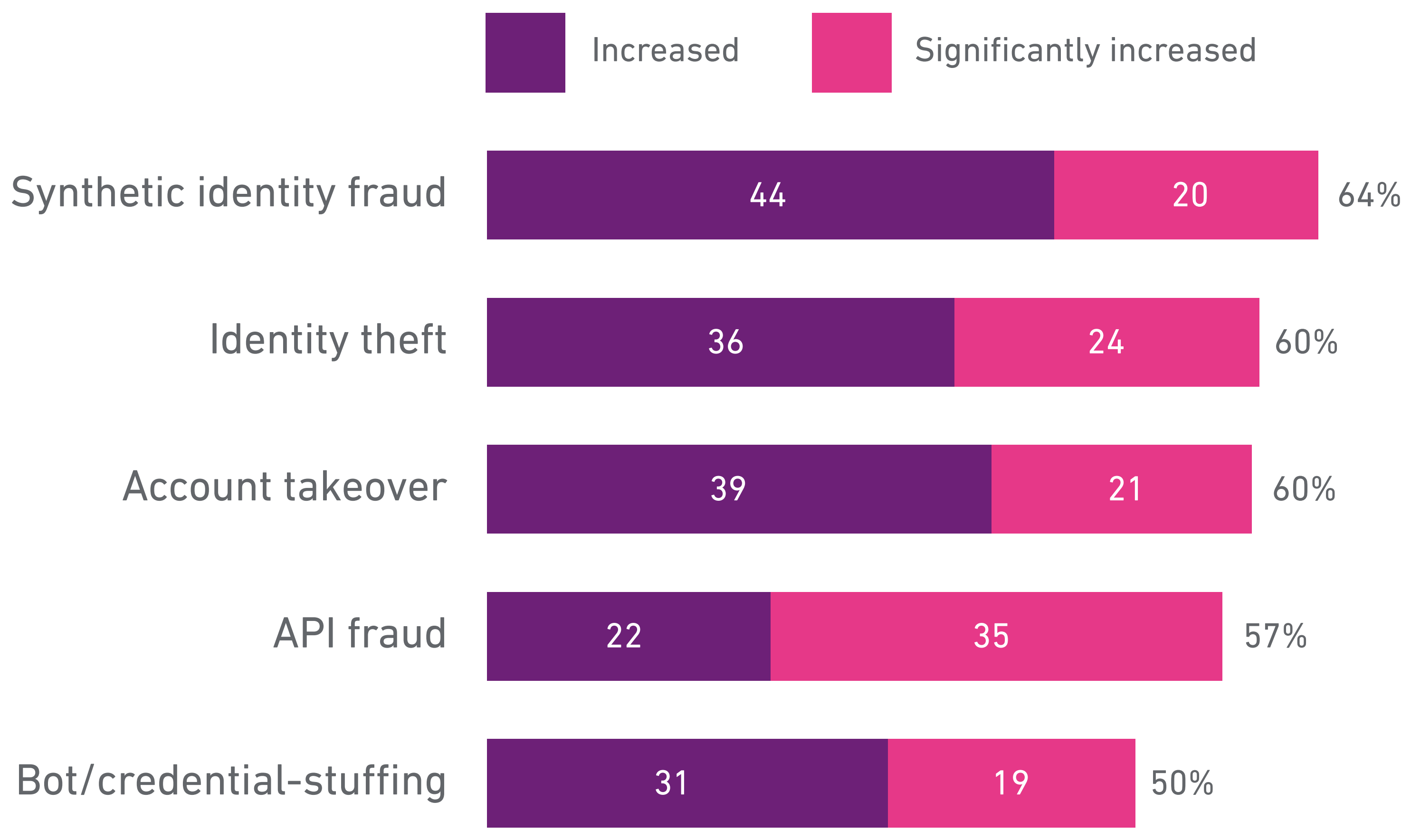
In the eCommerce sector, friendly fraud attacks have seen the biggest increase for 59% of merchants. This is likely to be a direct result of ongoing financial pressure on consumers. Many previously good customers may be tempted to be dishonest and claim chargebacks – especially considering the rampant spread of ‘tricks’ or ‘methods’ on social media that promote these techniques under a veneer of legality.

64% OF BUSINESSES

experienced an increase in synthetic identity attacks in the last financial year.

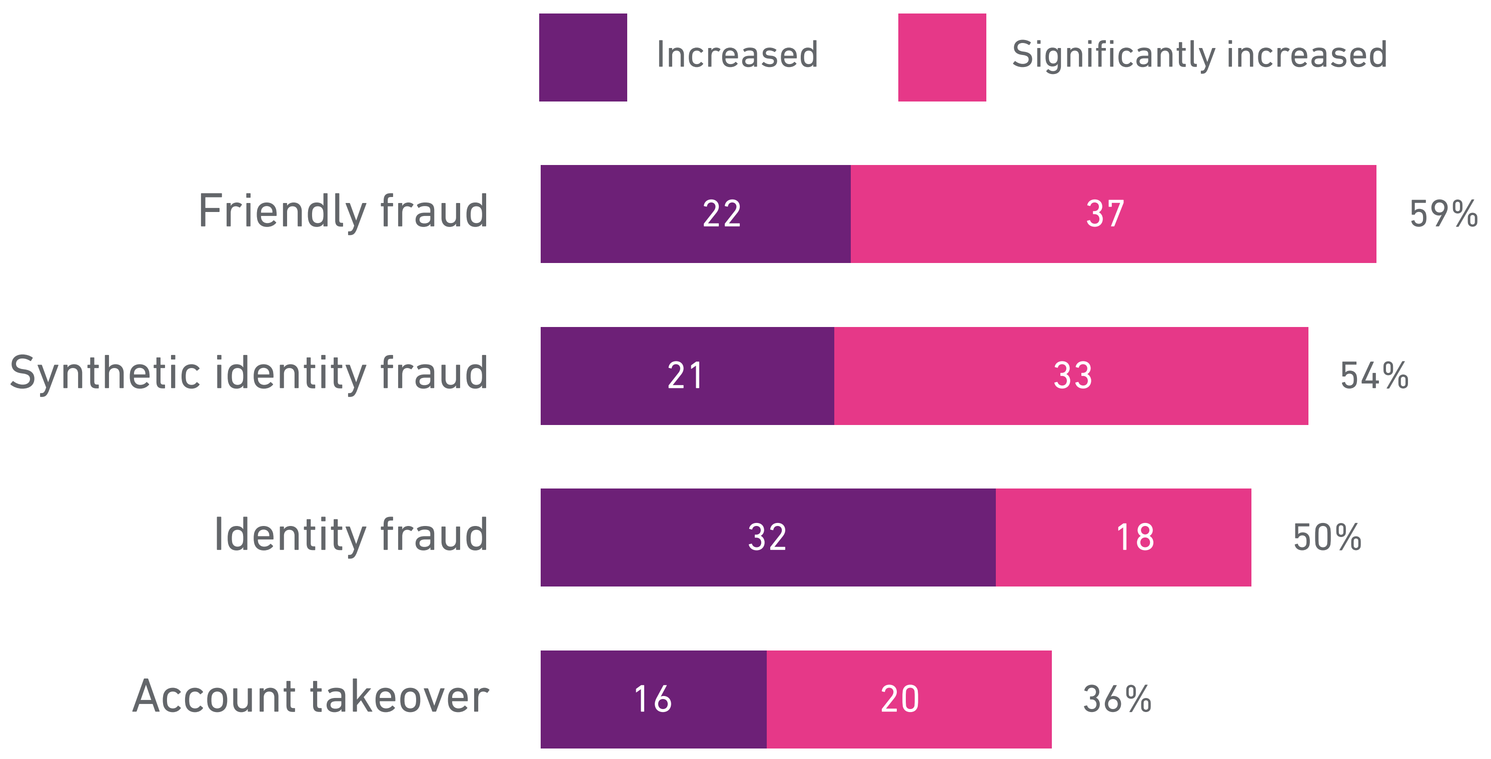
How has the volume of fraud attacks changed in the last financial year?

Financial Services and Telcos



Base: *216 EMEA & APAC fraud decision makers and Financial Services and Telco firms*
Source: *Experian research conducted by Forrester Consulting, July 2023*

eCommerce



Base: *92 EMEA & APAC fraud decision makers in eCommerce*
Source: *Experian research conducted by Forrester Consulting, July 2023*

57% OF FINANCIAL SERVICES

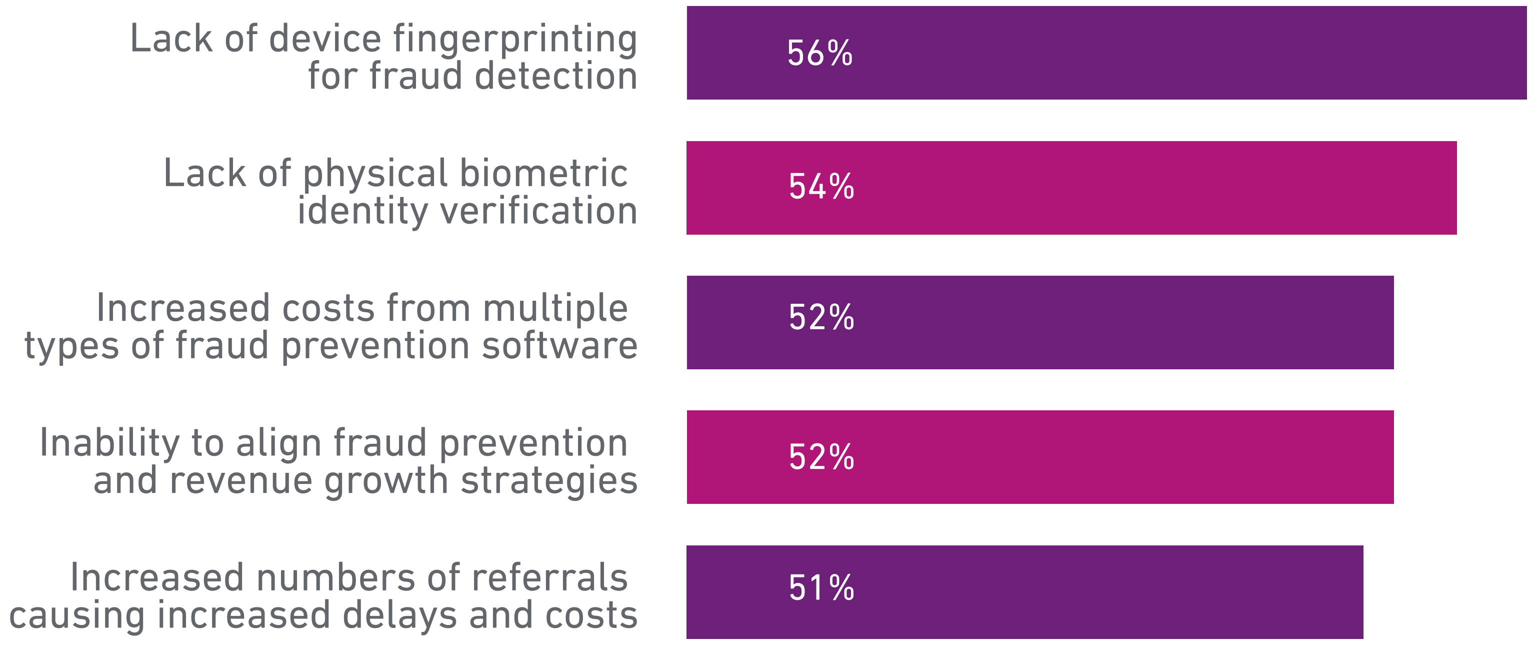
and Telco firms have seen an increase in API fraud attacks.

59% OF ECOMMERCE MERCHANTS

have seen an increase in friendly fraud.

FRAUD CHALLENGES AND PRIORITIES

Top 5 challenges limiting businesses' ability to prevent fraud



Base: *308 EMEA & APAC fraud decision makers at Financial Services, Telco and eCommerce firms*
Source: *Experian research conducted by Forrester Consulting, July 2023*

Top fraud challenges

FIRST CHALLENGE

Our research shows that the biggest gap in respondents' ability to prevent fraud is a lack of device fingerprinting (56%). So why has this capability possibly become the most essential layer in fraud prevention?

There are three main reasons:

- Firstly, device data can be monitored from the moment a customer opens a website. This allows for continual assessment of fraud risk before the customer completes an application or makes a purchase.
- Secondly, device intelligence is gathered completely passively, which means the user experience is unaffected and the customer can browse the website uninterrupted.
- Thirdly, although fake identities are now much easier to create, real customers have a digital history and AI cannot alter historical data – so analysing the data trail of each user has become a vital signal for fraud.

Essentially it comes down to the fact that the key to successful fraud prevention is data. But access to data is not enough, it must then be connected, analysed and constantly updated to create meaningful insights that can drive better decision making. This can only be achieved through the use of AI-powered analytics and ML.

SECOND CHALLENGE

The second biggest gap in fraud prevention capability is a lack of physical biometric identity verification (54%).

It is encouraging to see that many businesses are recognising that there is an urgent need to provide this layer of fraud prevention. A global **Experian survey of over 6,000 consumers** in 20 countries found that 81% of respondents believed that physical biometrics are the most secure method to verify their identity online.

Savvy business leaders recognise that providing facial recognition authentication benefits them on multiple fronts, as it enhances their reputation with customers, while also improving CX by reducing the friction associated with physical document checks.

81% HAVE CONFIDENCE IN PHYSICAL BIOMETRICS

THIRD CHALLENGE

Managing multiple types of fraud prevention software and the associated costs is the third biggest challenge limiting businesses' ability to prevent fraud (52%).

Nearly half of our respondents (46%) are using three or more fraud solutions, with the vast majority (92%) using a hybrid approach that includes solutions provided by external partners as well as those developed in-house.

As firms start to require more fraud software services to stay at pace with the fraud threat, it becomes much more important to manage and orchestrate those solutions in a connected way. Adding new fraud solutions brings complexity for IT teams. How will a new fraud check integrate with other existing fraud solutions and how will it impact user workflows?

46% ARE USING THREE OR MORE FRAUD SOLUTIONS

This is why organisations are turning to orchestration solutions to better connect and manage all their different identity and fraud services – bringing multiple platforms and solutions together in a more efficient way. This can simplify the complexity and reduce the costs associated with multiple specialised fraud tools by connecting them through a single, flexible API.

Top fraud priorities

Top 5 fraud-related priorities for the next 12 months

1 Improve explainability into ML decisions (58%)

2 Address bias in ML models (52%)

3 Reduce the number of platforms across the business (51%)

4 Reduce silos between multiple fraud platforms (48%)

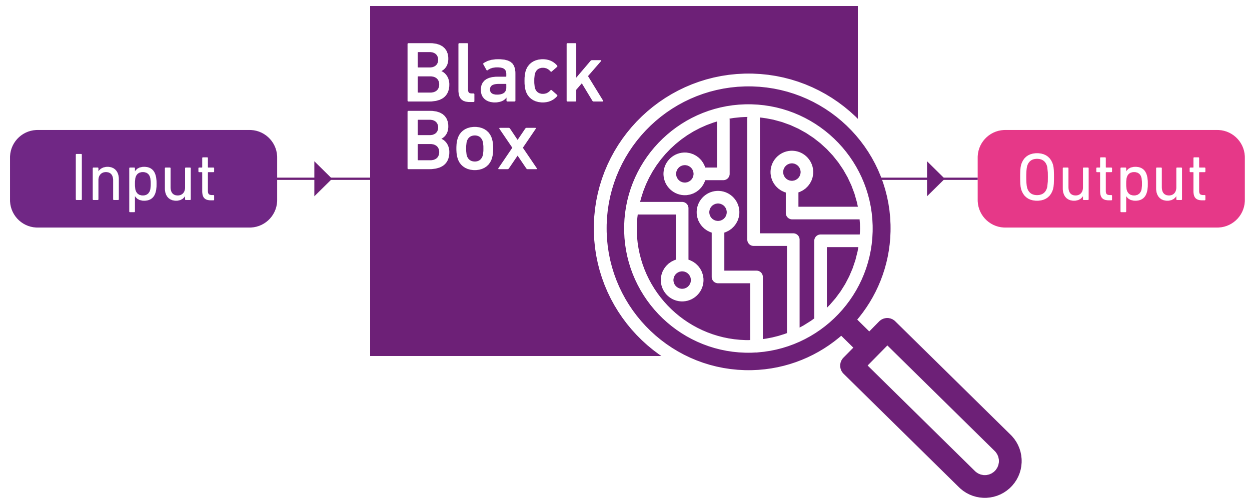
5 Reduced fraud losses (47%)

Base: 308 EMEA & APAC fraud decision makers at Financial Services, Telco and eCommerce firms
Source: Experian research conducted by Forrester Consulting, July 2023

74% OF RESPONDENTS BELIEVE THAT

ML-based fraud detection is the most effective way to prevent fraud.

The top two fraud-related priorities highlight how important ML has become to fraud prevention. **Improving the explainability of ML models** (58%) **and addressing bias in ML models** (52%) are closely linked as transparent ML models allow for unintentional bias to be identified. It is interesting to note that these two factors align closely with our recent **AI research into credit risk assessment**.



Apart from the fact that explainable ML is likely to be a requirement under a future AI legal framework, there are multiple benefits that explainability can provide:

- Transparency enables human oversight so that data scientists and developers can diagnose model degradation issues and resolve them.
- Analysing the impact of each contributing feature in a model allows for any bias to be identified and removed to ensure that models are not unintentionally discriminatory.
- When employees can understand the contributing factors of a fraud risk score it helps to build trust in the models' capability.

Transparent and explainable use of ML is clearly a priority as organisations bet on this technology as the future of fraud prevention.

THREE

Fighting fire with fire

FIGHTING FIRE WITH FIRE

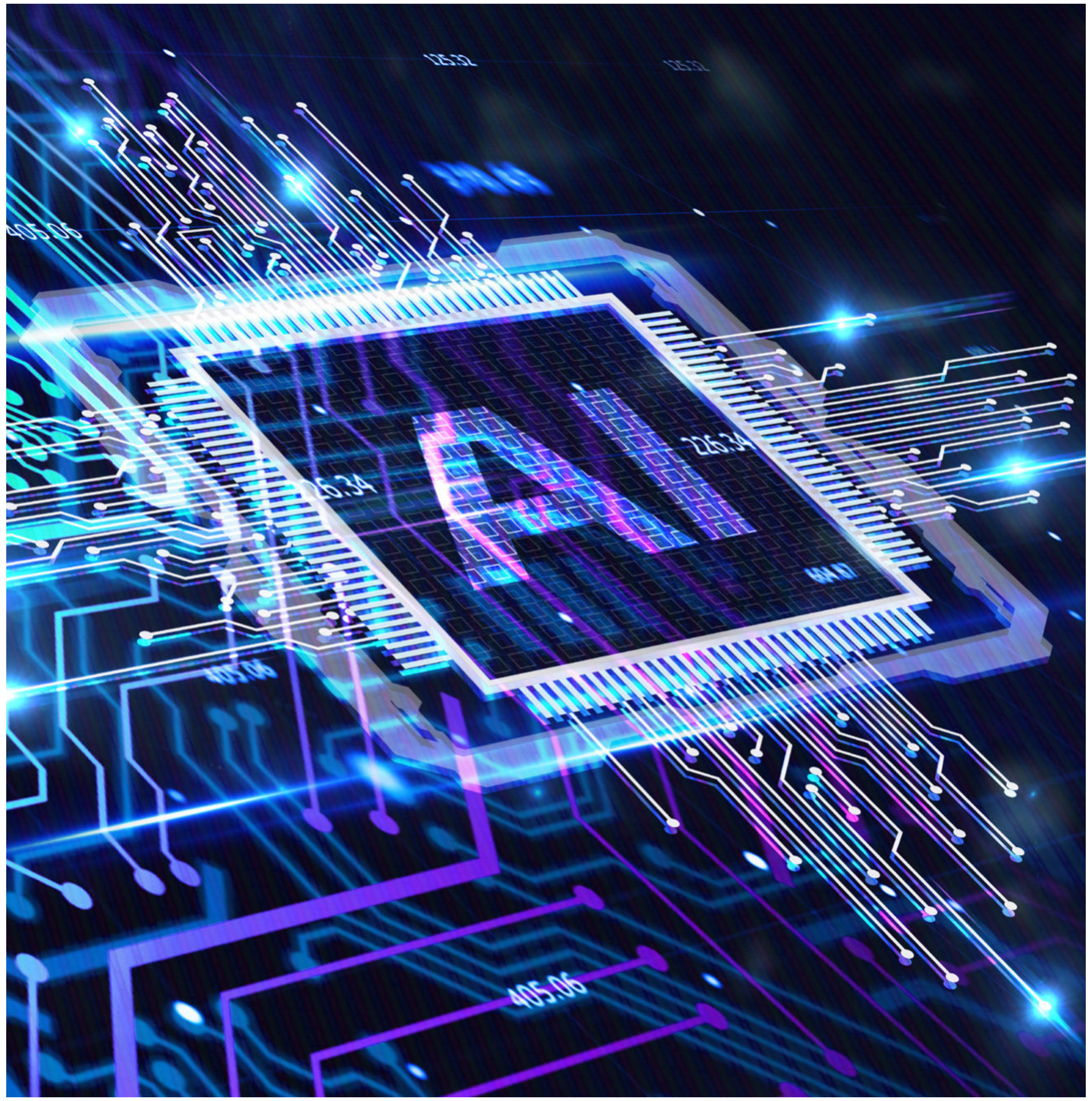
There is no way we can reverse publicly accessible GenAI - Pandora's box has been opened. It is likely that in years to come this high-impact technology will be seen as a watershed moment that changed the fraud landscape forever.

Although the fraud threat is intensifying on several fronts, fraud prevention technology is also constantly improving – largely due to innovations driven by AI.

By using a layered approach that includes physical and behavioural biometric identity verification, device intelligence data and ML in a continuous evaluation across user sessions, businesses can defend themselves while still providing good customers with minimal friction.

And as the layering of fraud defences becomes more important, so does the need to manage and orchestrate multiple fraud solutions. Accomplishing this can best be achieved by using smart orchestration, which enables the configuration of automatic, predefined customer journeys based on the desired risk appetite.

This means that different users will experience a different journey with relevant identity and fraud services called up dynamically, based on the specific journey workflow. This prevents a one-size-fits-all approach, where every customer must pass through the same steps, which in turn leads to increased abandonment.

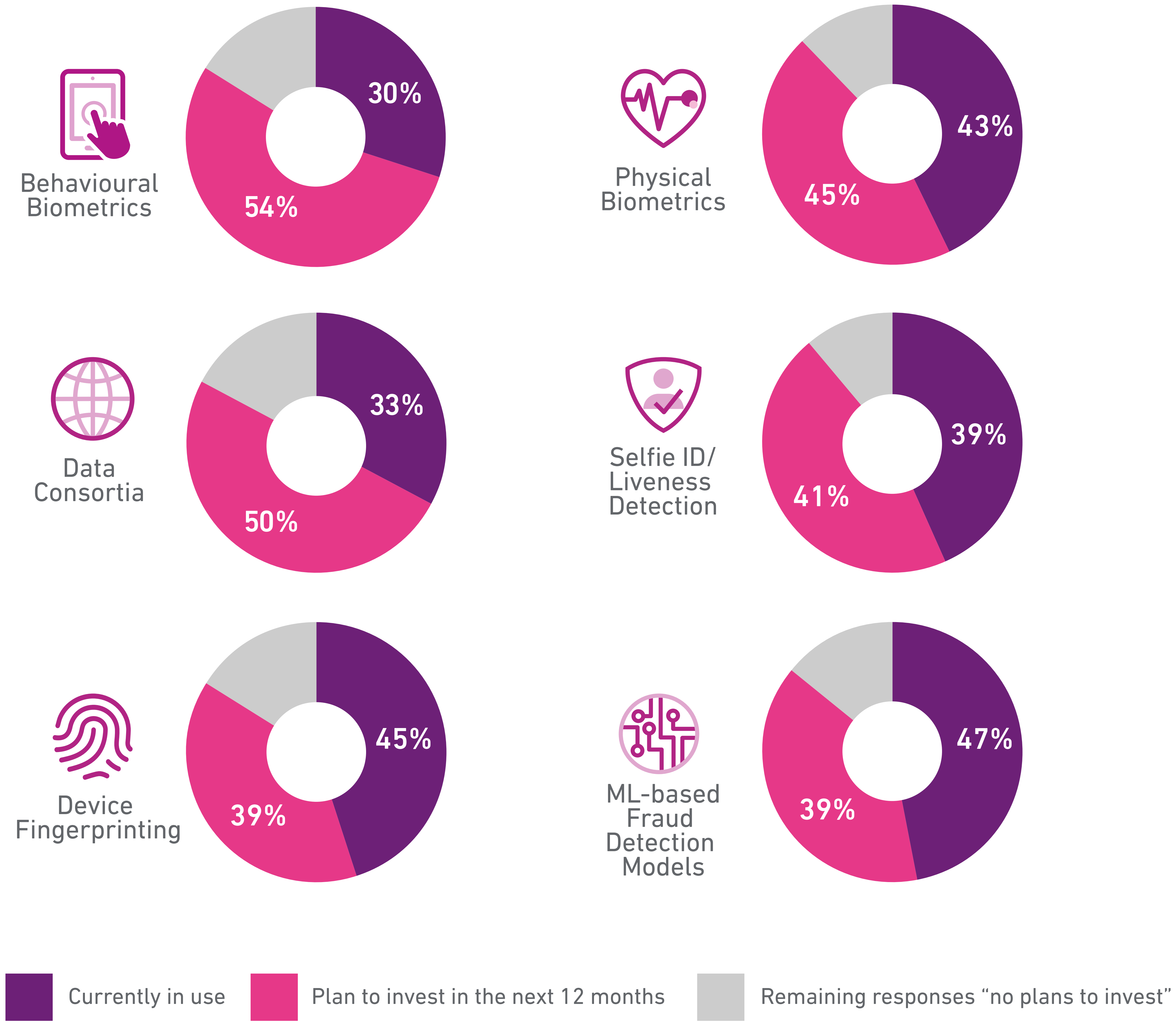


The move to passive fraud prevention

Looking at current and future fraud prevention measures it is clear that many businesses are planning to introduce passive fraud checks that can be continuously monitored from the moment a customer lands on their website. Device intelligence, which combines behavioural biometrics with device data and ML analysis, can reliably identify fraudsters without interrupting the customer journey.

Nearly two thirds (65%) of the fraud decision makers in our survey are prioritising passive fraud checks. These businesses recognise that passive controls can improve fraud detection accuracy while also enhancing customer experience, with less friction for good customers.

Snapshot of current and future fraud prevention measures



Base: 146 EMEA & APAC fraud decision makers at Financial Services, Telco and eCommerce firms
Source: Experian research conducted by Forrester Consulting, July 2023

The fraud prevention layer cake

No fraud prevention technology is infallible. However, when multiple technologies are used together, they provide a much stronger defence than individually. The best fraud solutions **create enough challenges for an attacker that they decide that it is not worth their time**.

A combination of active and passive fraud checks that can be activated based on the user journey (for example the login vs. application process) can greatly improve fraud detection accuracy, and with the introduction of ML, can reduce the volume of manual reviews and false positives. Let's take a closer look at the different layers required for effective fraud prevention.

LAYER 1 = AI AND ML

Our research shows that ML has become an essential element of every fraud prevention strategy, with close to three quarters (74%) of respondents stating that ML-based fraud detection is the most effective way to prevent fraud. This is unsurprising considering the improvements that this technology provides over traditional rules-only approaches and the emergence of AI-powered fraud.

One of the biggest benefits of ML is that it can near-instantly analyse huge volumes of data to detect anomalies and identify patterns that would not be apparent to a human fraud specialist. Another advantage is that rather than producing a binary yes/no recommendation, ML-driven solutions provide a fraud risk score that allows businesses to precisely set their risk appetite.

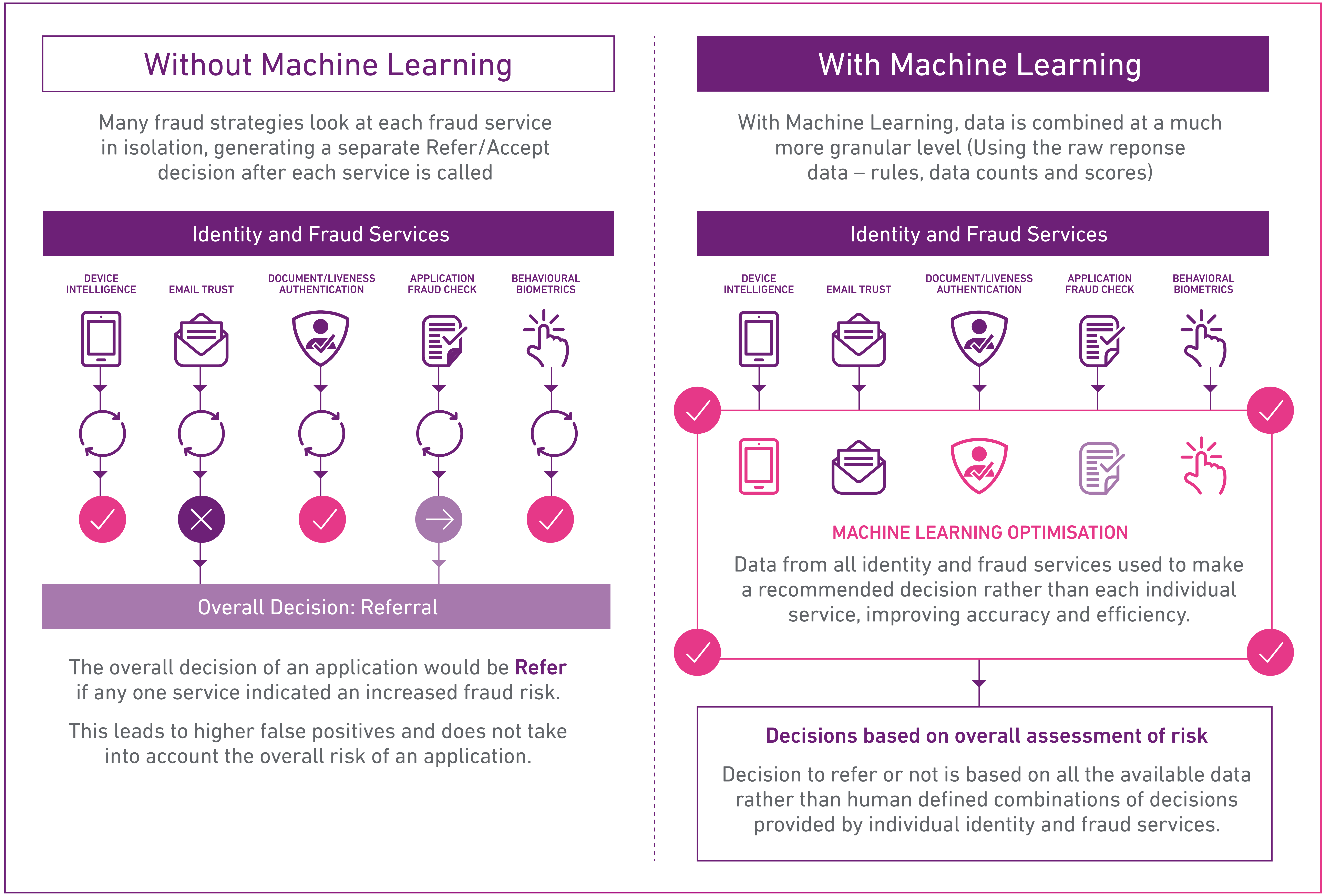
Perhaps the most important benefit of ML-based fraud prevention is the capacity to continually learn from previous fraud cases. As more data is added to the model over time, it becomes more and more accurate at classifying fraudulent cases. This is vital for businesses to rapidly respond to changing fraud patterns and ensure that they stay at the cutting edge of fraud prevention.

ML can now be applied in a number of different ways. It can form the basis of a fraud model, be used to uncover new fraud patterns in order to update rules or be used within the software that powers an individual fraud solution. And it can also be used to evaluate recommendations from multiple services to make a more accurate overall assessment of fraud risk. This is particularly important when multiple identity and fraud services are required as part of the same process, for example in customer onboarding.

79% OF BUSINESSES

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

ML provides a more accurate overall fraud decision



Without Machine Learning

Many fraud strategies look at each fraud service in isolation, generating a separate Refer/Accept decision after each service is called

Identity and Fraud Services

Overall Decision: Referral

The overall decision of an application would be **Refer** if any one service indicated an increased fraud risk.

This leads to higher false positives and does not take into account the overall risk of an application.

With Machine Learning

With Machine Learning, data is combined at a much more granular level (Using the raw reponse data – rules, data counts and scores)

Identity and Fraud Services

MACHINE LEARNING OPTIMISATION

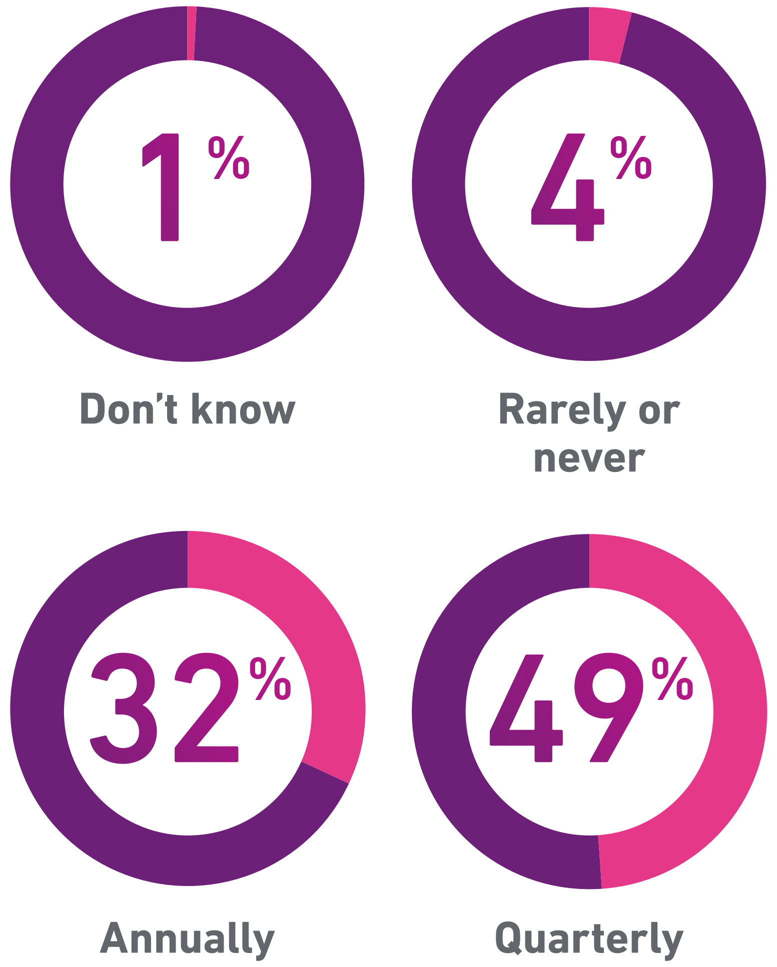
Data from all identity and fraud services used to make a recommended decision rather than each individual service, improving accuracy and efficiency.

Decisions based on overall assessment of risk

Decision to refer or not is based on all the available data rather than human defined combinations of decisions provided by individual identity and fraud services.

The ability to stay at pace with new fraud threats is highly dependent on how often businesses update their ML fraud prevention models. It is concerning that only 14% of those using ML transactional fraud models update them monthly or more frequently. Nearly a third (32%) are only updating their models annually. This update frequency exposes businesses to considerable risk from new fraud attack vectors.

How often do businesses that are already using ML transactional fraud prevention models update them?



Base: 146 EMEA & APAC fraud decision makers at Financial Services, Telco and eCommerce firms
Source: Experian research conducted by Forrester Consulting, July 2023

LAYER 2 = PHYSICAL BIOMETRICS

ML also provides the analytical backbone for biometrics. These are a vital component of a layered fraud prevention strategy, as indicated by the 77% of respondents that believe biometrics is the most effective way to verify customer identity. Despite the sophistication of deep fakes created via GenAI, these forgeries are not yet available in real-time and facial recognition that uses liveness detection is still highly effective at authenticating identity.

The remarkable development in deep fakes means that they are now indistinguishable to the human eye. However, the latest liveness detection technology can identify if images are presented on a screen, rather than a physical person, by analysing subtle colour hues and even detecting heartbeats. A necessary additional layer of security can be achieved from active and spontaneous liveness checks like smiling or moving the head in a certain way on request.

45% OF BUSINESSES PLAN TO

invest in physical biometrics in the next 12 months.

TO FIND OUT MORE ABOUT ML FRAUD PREVENTION READ OUR COMPREHENSIVE GUIDE →

LAYER 3 = DEVICE INTELLIGENCE

Device intelligence is another critical component of fraud prevention, as recognised by the 73% of respondents who agree that device fingerprinting is a must-have. As with biometrics, the analytical core of device intelligence is provided by ML algorithms. The benefit of this technology is that every device has a historical data trail that is very hard to manipulate.

The latest device fingerprinting tools can analyse over 150 different attributes related to a customer's device and network to provide a comprehensive connection between their device and their identity. Rather than a one-off authentication, these attributes can be continually monitored throughout each session. This continuous passive authentication can improve the accuracy of fraud detection considerably without any negative impact on customer experience.

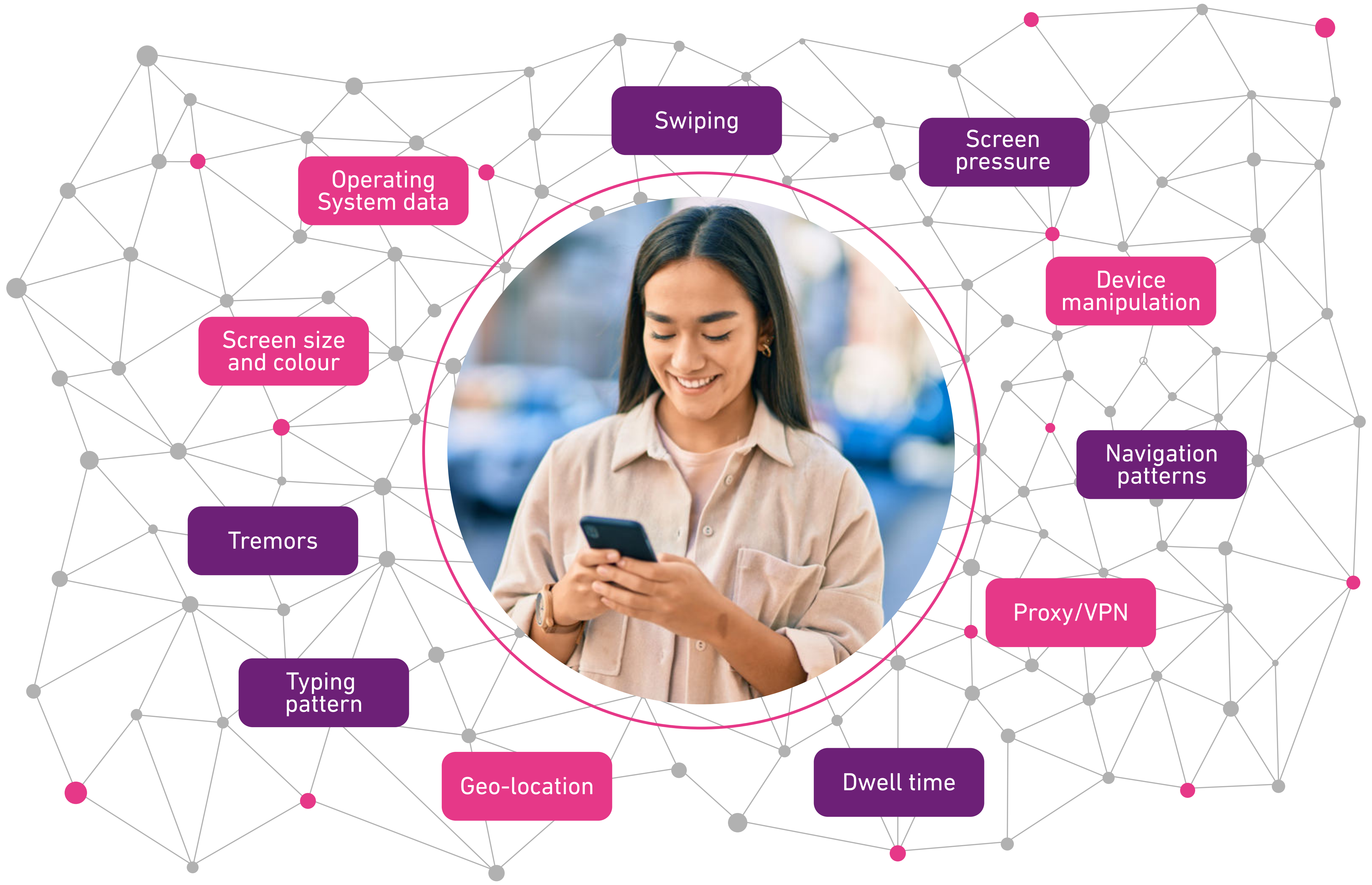
As physical biometrics are threatened by advances in GenAI, wise businesses are looking to expand their use of behavioural biometrics, with 54% of respondents planning to invest in this technology in the next 12 months. Behavioural biometrics are virtually impossible for fraudsters to replicate as they rely on unique, subconscious behavioural patterns. These are extremely difficult to imitate and can be analysed continuously and passively during a user session.

54% OF BUSINESSES PLAN TO INVEST

in behavioural biometrics in the next 12 months

Device intelligence has become a high priority

Device fingerprinting and behavioural biometrics can increase detection without impacting the customer experience.



LAYER 4 = RULES

Although ML has become indispensable to fraud prevention, the most effective solutions use ML in conjunction with rules. ML-based solutions allow you to greatly reduce the number and complexity of rules, but business specific rules are still very important and continue to complement other fraud systems in a variety of ways. The latest no-code, drag-and-drop rule engines allow users to test the impact that a new rule will have before introducing it to a live environment.

Another important function of rules is that they can be proactively created based on fraud intelligence received from other businesses within a consortium. Rather than reacting to fraud, this puts businesses on the front foot to prevent new fraud techniques as soon as they are identified by their associates.

LAYER 5 = FRAUD CONSORTIA

Fraud prevention is best achieved via collaboration and as the fraud threat intensifies, data sharing between organisations is becoming increasingly necessary. According to our research, 50% of businesses are planning to invest in consortia data in the next twelve months to boost their fraud detection ability. A similar number of respondents (48%) agree that anonymised fraud data sharing between organisations will help to tackle the fraud problem.

There are numerous benefits to fraud consortiums, including:

- By pooling data, each business gains a more comprehensive view of fraud trends and patterns than from their own data alone.
- Consortium members receive real-time alerts about suspicious activities, helping them take immediate action and pre-emptively prevent fraud.
- Smaller businesses benefit from the collective strength of the consortium by accessing resources and insights that might otherwise be out of reach.
- Many regulatory bodies encourage participation in fraud consortiums as a means of complying with due diligence requirements in preventing financial crimes.

UNPACKING AI-POWERED FRAUD PREVENTION

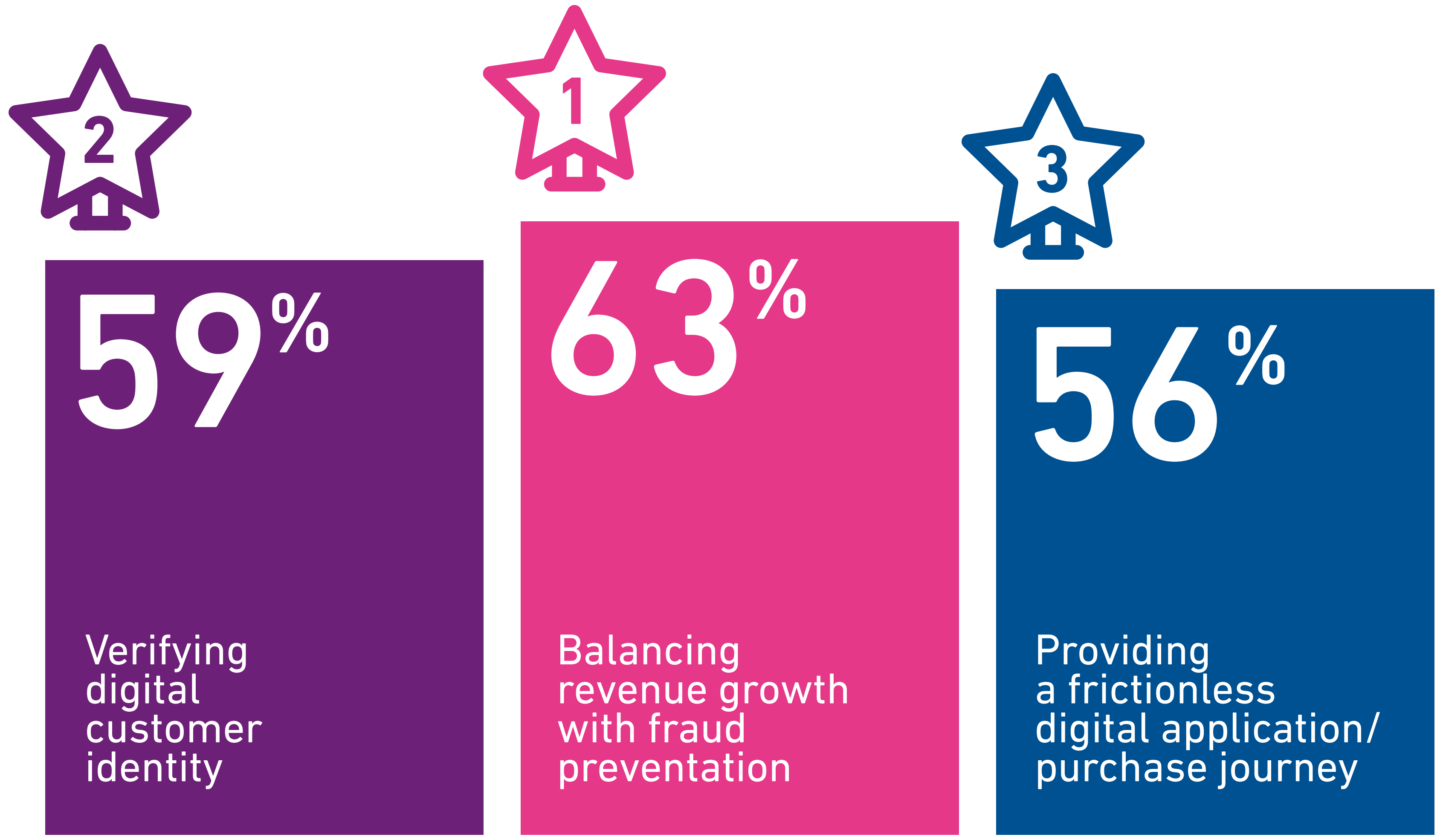
To understand why businesses are turning to AI/ML it is helpful to look at the top three fraud-related issues in regard to digital customer experience (CX).

The most challenging issue is verifying digital customer identity (63%), this is followed by balancing revenue growth with fraud prevention (59%) and lastly, providing a frictionless digital application journey (56%). So how can ML address these issues?

71% OF FIRMS BELIEVE

that the future of fraud prevention will be driven by AI/ML-based solutions.

Top three fraud-related challenges related to digital CX



Base: 308 EMEA & APAC fraud decision makers at Financial Services, Telco and eCommerce firms
Source: Experian research conducted by Forrester Consulting, July 2023

Verifying digital customer identity

Authenticating new customers requires a delicate balance to avoid them abandoning the application or purchase. Only 20% of our respondents believe that their fraud prevention strategy has a minimal impact on their customer abandonment rates, with the majority (78%) believing that it has a noticeable impact.

Let's look at how ML can help businesses verify digital identity:

Instant document verification

Models can be trained to extract, scan and validate various types of identity documentation provided by the customer. Collected personal identification data can be assessed against third-party sources. Optical character recognition (OCR) data can also be used to prepopulate forms which reduces onboarding time for the customer.

Facial recognition with liveness detection

Compare the customer's photo on their ID document with a selfie or liveness check to confirm their identity and verify that they are physically present in a matter of seconds. ML algorithms analyse facial features from images or videos to identify unique characteristics associated with the customer.

Biometric behavioural analysis

Analyse the user's behaviour patterns, such as typing speed and mouse movements, and create a profile for each user to simplify the verification of returning customers and reduce the risk of bot attacks.

Device fingerprinting

Each device has a unique set of characteristics, such as IP address, browser type, geolocation and operating system that can be used to create a device fingerprint associated with each customer. Analysing the device's interaction history allows for the identification of suspicious activity linked to account takeover or identity fraud.

By implementing these measures, businesses can ensure that their digital customer verification is sufficiently robust while still providing a smooth customer experience. The benefits of ML go beyond fraud prevention, as automating fraud risk assessments means that good customers can pass through these checks quickly – reducing the time to decision and improving CX.

70% OF OUR RESPONDENTS BELIEVE THAT

the ability to automate more decisions for legitimate customers is an important factor when considering an ML-based fraud prevention solution.

78% OF BUSINESSES BELIEVE THEIR

fraud prevention strategy impacts their customer abandonment rate.

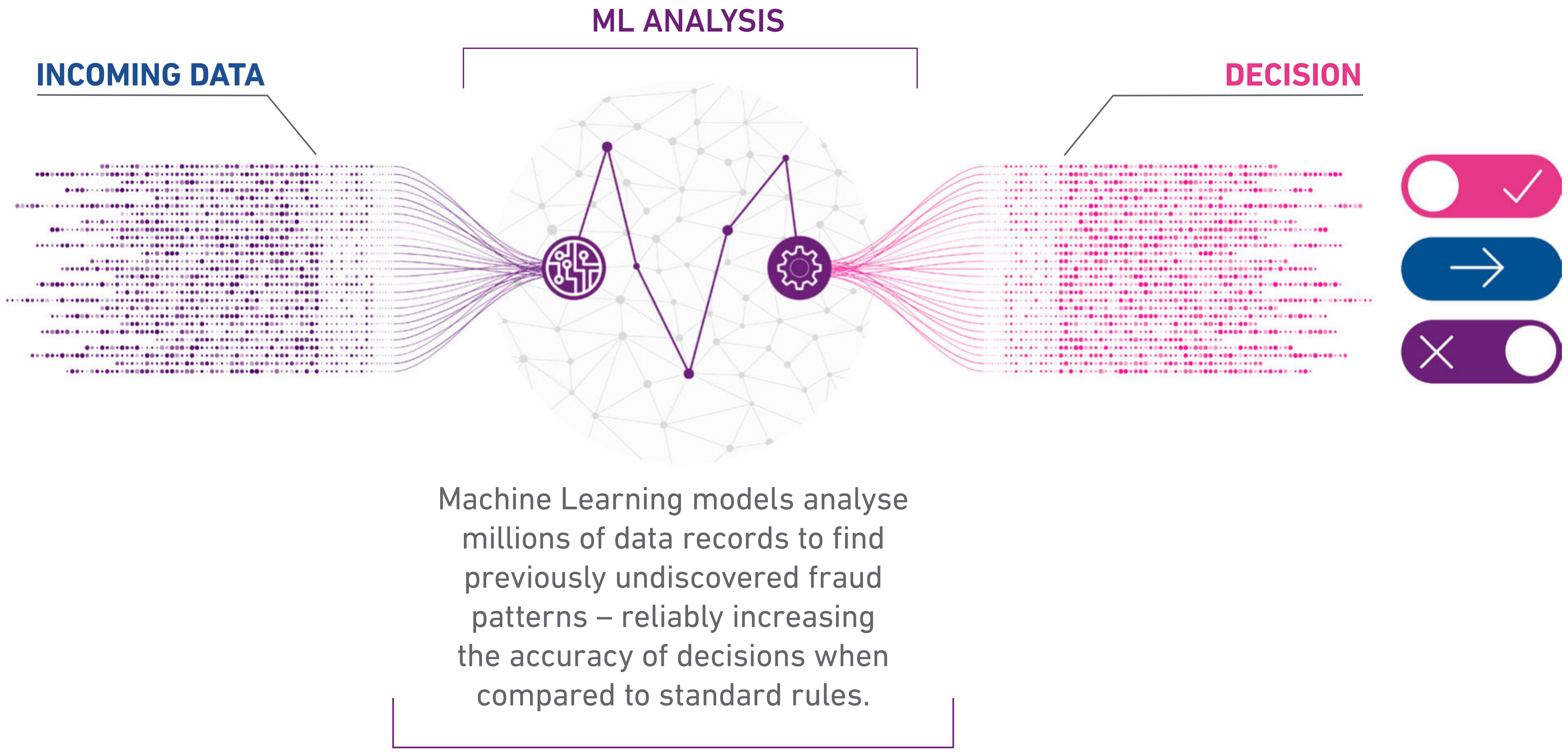
Balancing revenue growth with fraud prevention

The inability to align fraud prevention with revenue growth strategies is one of the biggest challenges that many businesses face. At the heart of this issue is the problem of false positives. Overly strict and outdated fraud prevention rules with rigid parameters mean that genuine customers are incorrectly declined if a single data point is outside of the normal framework. But at the same time, if fraud prevention rules are relaxed, then fraud losses increase.

According to our research, 70% of businesses find that false positives cost their business more than fraud losses. Nearly three quarters of our respondents are leaving more money on the table than what they lose to fraud!

When you consider that the impact of false positives goes beyond the immediate loss and has ongoing ripple effects – which include customer frustration, service centre expenditure, wasted marketing budget, potential loss of future sales and ultimately damage to a business's reputation – the severity of this problem becomes even more apparent.

The best way to address this issue is by using ML to improve the accuracy of fraud prevention so both fraudsters and legitimate customers can be better identified. ML enables a wider analysis of data points than rule sets. The result is a more comprehensive assessment that won't block a transaction or application due to a single errant data point, instead providing a more nuanced recommendation. The latest **ML-powered fraud prevention solutions** can accurately identify 99.9% of all transactions, which can result in up to 15% more revenue – due to a reduction in false positives.



Machine Learning models analyse millions of data records to find previously undiscovered fraud patterns – reliably increasing the accuracy of decisions when compared to standard rules.

For many years false positives have been accepted as an inevitable consequence of traditional rules-based fraud prevention systems. Our research shows that 41% of businesses do not even track false positives and therefore do not understand the full impact they have on revenue. The performance uplift that can be gained from ML models requires a change in thinking, with the new goal being the drastic reduction of false positives.

Providing a frictionless digital application journey

Consumers have more options and less patience than ever before. According to our **research study of over 3,000 consumers** in the EMEA region, 58% had abandoned an application in the previous year due to a lengthy, complicated process. This illustrates how important it is to reduce friction via automated identity and fraud checks.

The biggest spanner in the works of digital onboarding or checkout purchases occurs when applications or transactions trigger manual reviews. During peak traffic events – such as the launch of a new product or special offer – these manual assessments can overwhelm fraud teams and result in significant delays in processing flagged transactions.

ML can address this issue in a number of ways:

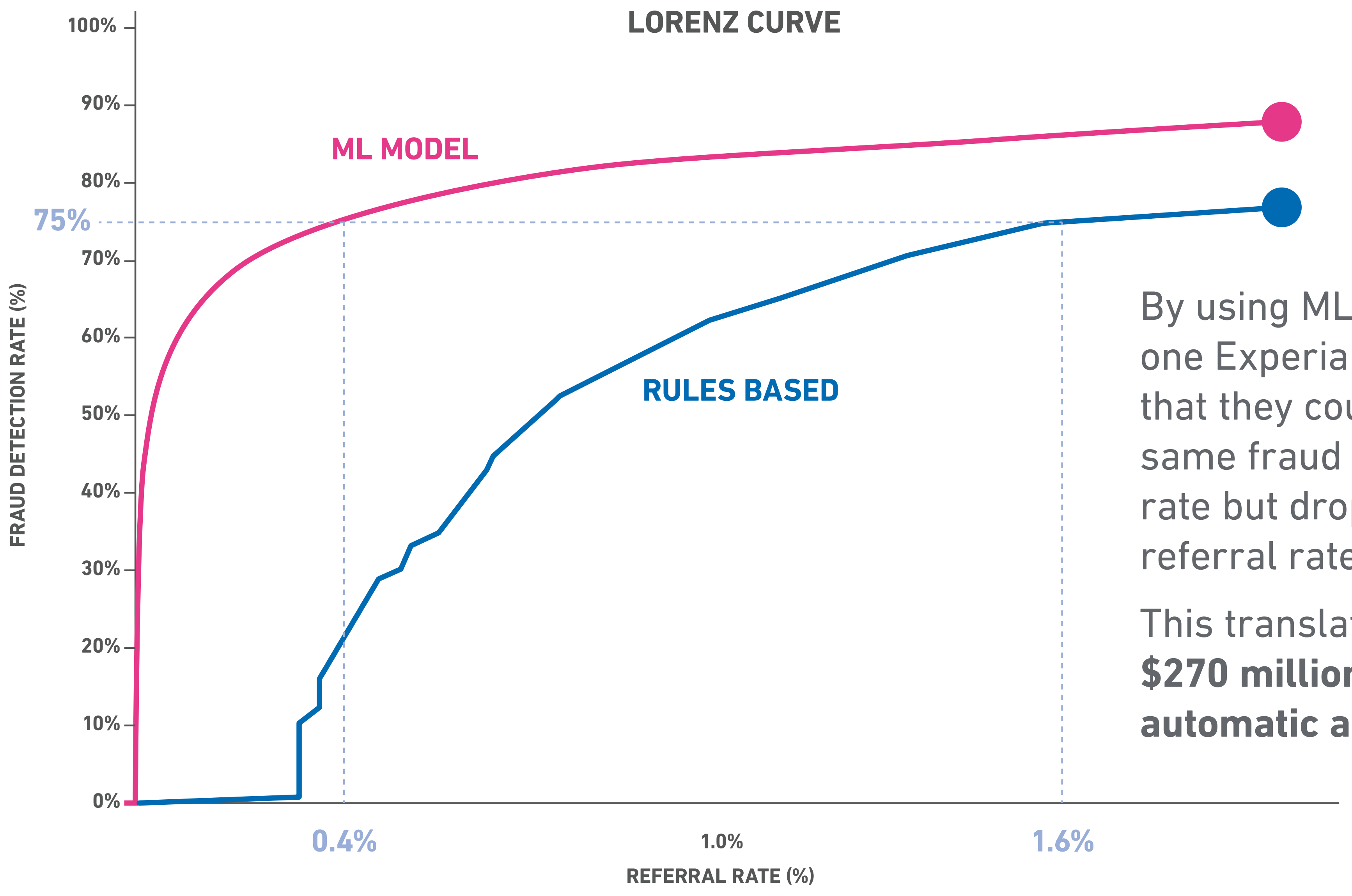
- **Faster detection** – automated recommendations are provided in 400 milliseconds or less so transactions can be classified almost instantly.
- **Improved accuracy** – means fewer transactions are flagged for manual review, as experienced by an Experian client that reduced their referral rate by 74%.
- **Scalability** – manage long-term growth and high-sales events without backlogs or the need for additional fraud agents.
- **No downtime** – unlike human specialists, ML delivers the same level of performance every day and night of the year.

Slashing the volume of manual reviews not only improves CX by near instantly processing transactions but also reduces the workload for fraud specialists. Considering these benefits, it is unsurprising that 71% of fraud decision makers believe that a reduction of manual reviews for their fraud agents is an important factor when considering an ML-based fraud prevention solution.

74% REDUCTION IN REFERRAL RATE

when introducing ML into fraud decisioning.*

ML reduces referral rate without impacting fraud detection



By using ML optimisation one Experian client found that they could keep the same fraud detection rate but drop their referral rate **by 74%**.

This translated to **$270 million of automatic approvals.**

**Based on Experian client data*

FIVE

Key takeaways

KEY TAKEAWAYS

1

73% of businesses have seen an increase in fraud losses over the past year, with 50% expecting losses to increase over the next 12 months. This future prediction may be conservative, given the growing impact of GenAI in lowering technical barriers to fraud attacks and improving the quality of social engineering attacks.

2

A lack of device fingerprinting and physical biometrics is undermining businesses' ability to prevent fraud. Accordingly, a significant proportion of respondents plan to invest in these technologies over the next 12 months.

3

Nearly three quarters (72%) of businesses believe that the future of fraud prevention will be driven by AI/ML-powered solutions. The main benefits of using ML fraud solutions are an increase in acceptance rates, reduced losses through greater fraud detection accuracy and a reduction in the volume of false positives and manual reviews.

4

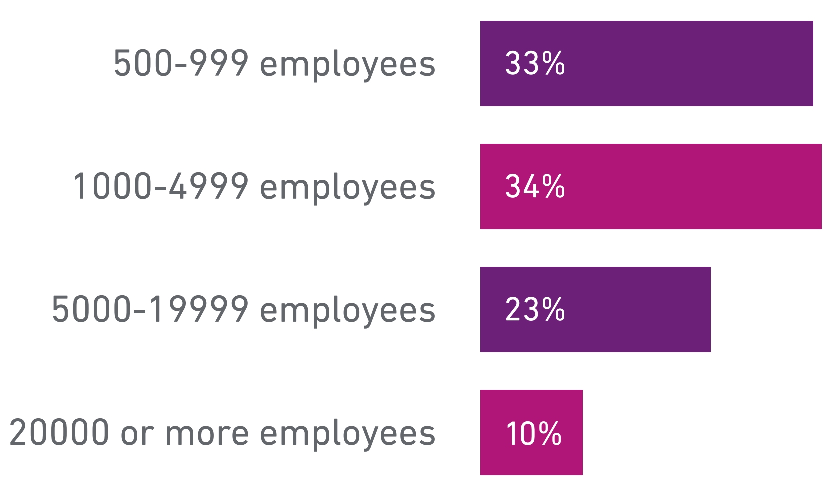
The top fraud-related priorities for the next 12 months are to improve the explainability of ML models and address unintentional bias in models. As businesses look to invest in ML-powered fraud prevention, it is essential that models are transparent to enable human oversight. This allows for bias removal, diagnostics for long-term model improvements and compliance with potential future regulations.

SIX

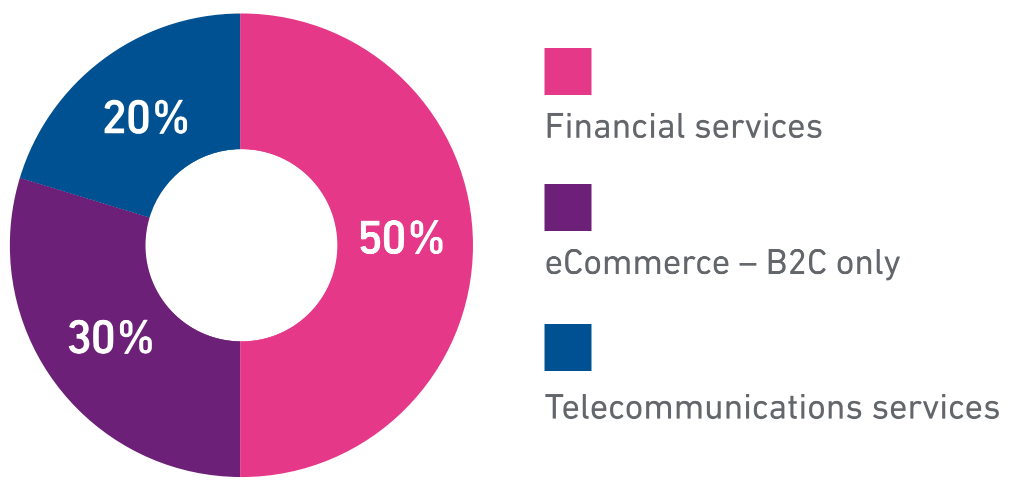
SURVEY FIRMOGRAPHICS

Total	N=308
Australia	N=24
Denmark	N=34
Germany	N=34
India	N=34
Italy	N=34
New Zealand	N=12
Netherlands	N=34
South Africa	N=34
Spain	N=34
Turkey	N=34

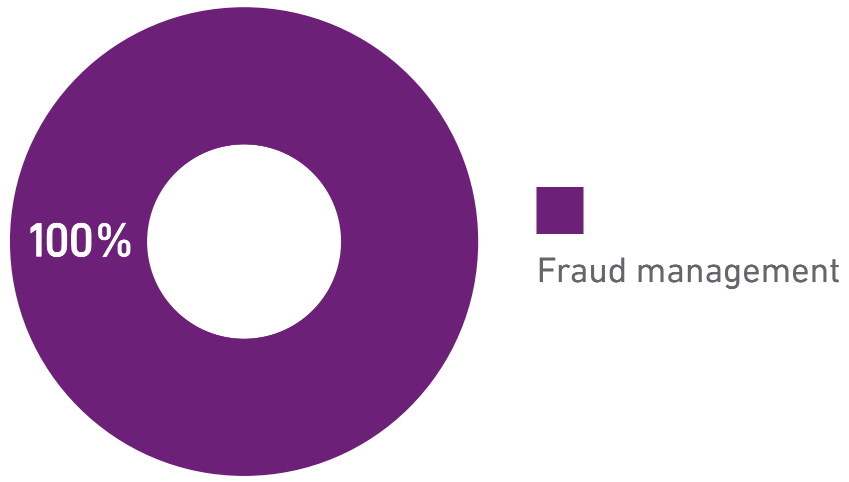
Company size



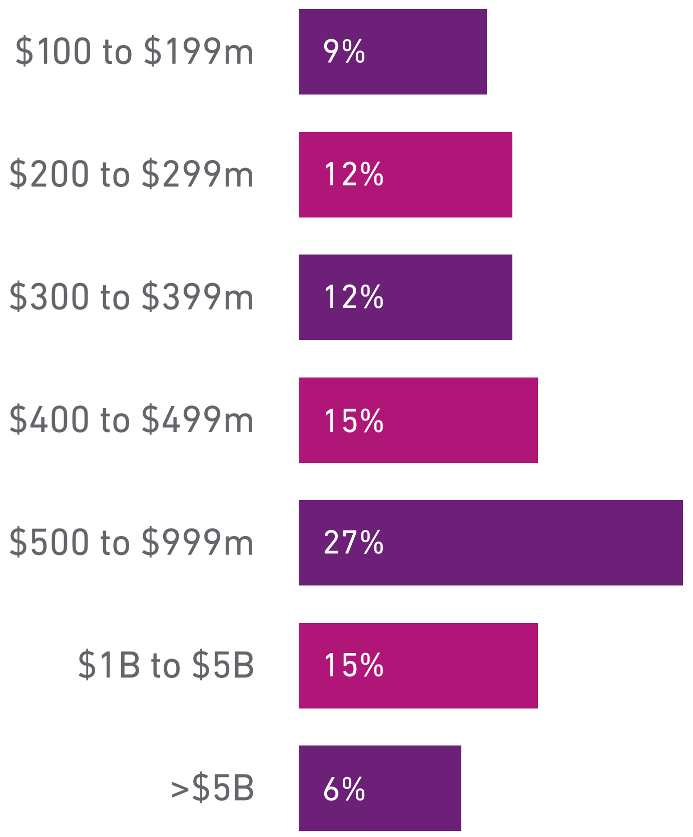
Industry



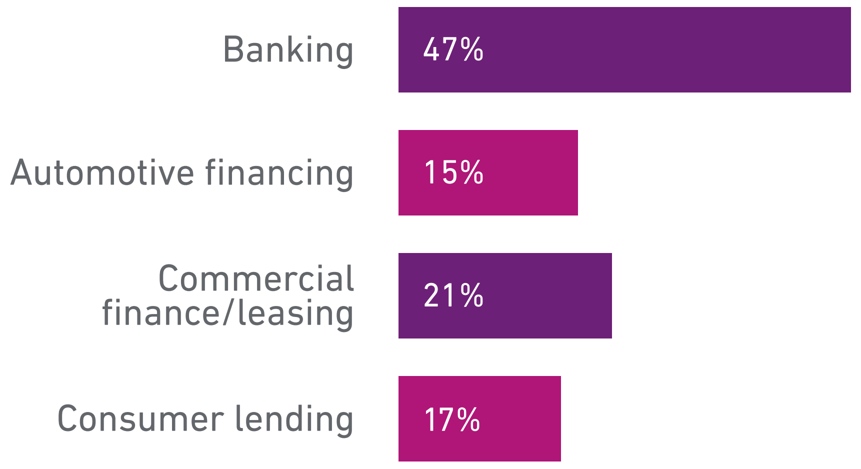
Job function



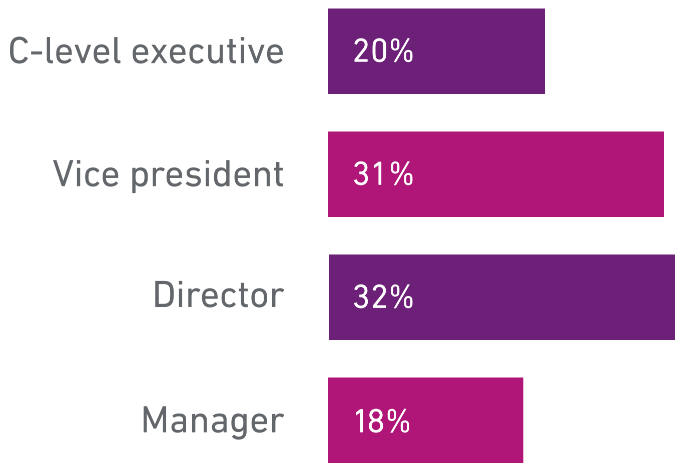
Revenue



Financial sector N=154



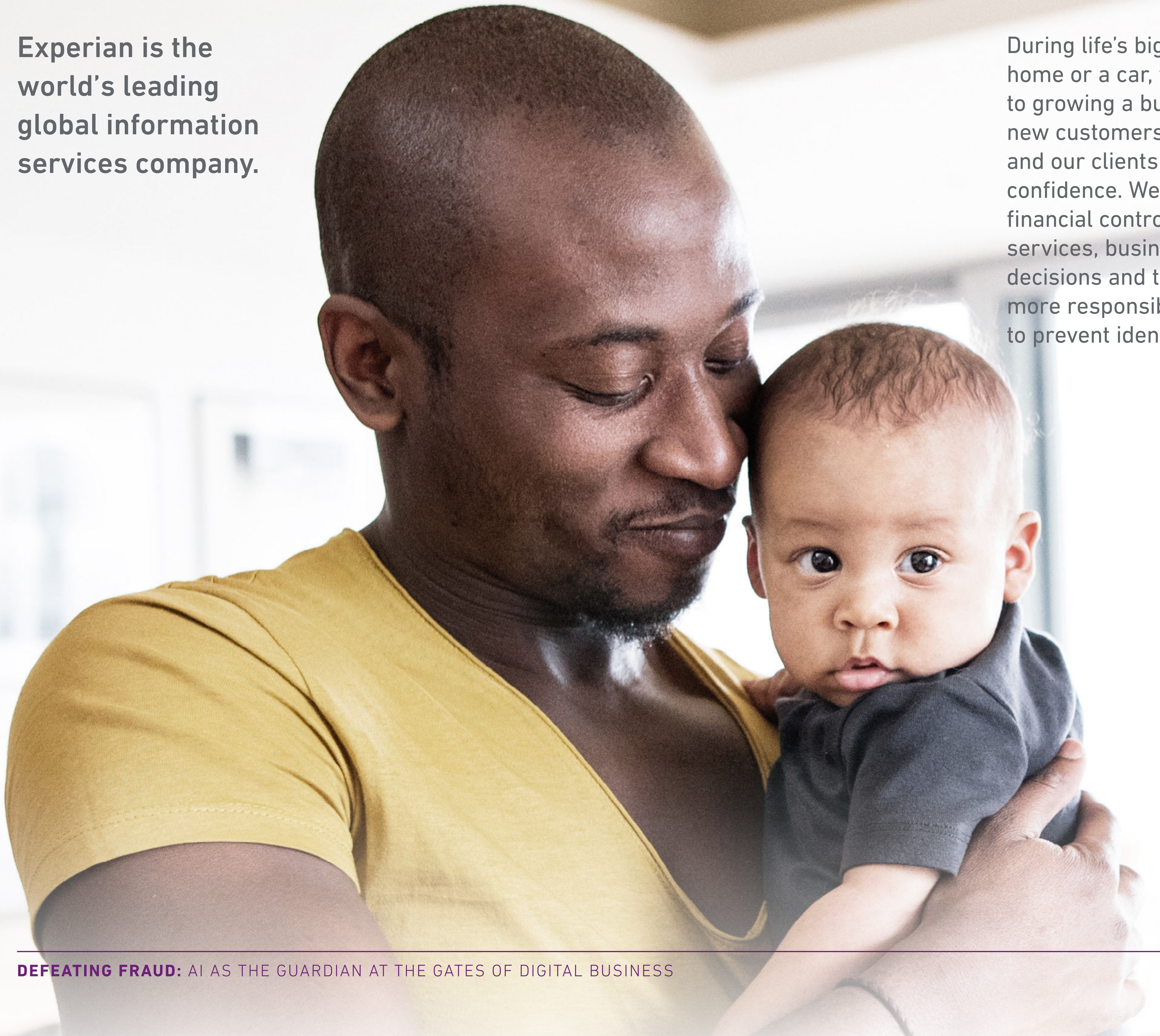
Job position



Survey firmographics

ABOUT EXPERIAN

Experian is the world's leading global information services company.



During life's big moments – from buying a home or a car, to sending a child to college, to growing a business by connecting with new customers – we empower consumers and our clients to manage their data with confidence. We help individuals to take financial control and access financial services, businesses to make smarter decisions and thrive, lenders to lend more responsibly, and organisations to prevent identity fraud and crime.

22,000

We have **22,000 people** operating across **32 countries**, and every day we're investing in new technologies, talented people, and innovation to help all our clients maximise every opportunity. With corporate headquarters in Dublin, Ireland, we are listed on the London Stock Exchange (EXPN) and are a constituent of the FTSE 100 Index.

LEARN MORE AT EXPERIANPLC.COM →

VISIT THE EXPERIAN ACADEMY →