PROACTIVE DEFENCE

Tackling evolving fraud threats

WELCOME TO EXPERIAN'S 2025 FRAUD REPORT

SHAIL DEEP
COO Experian EMEA & APAC

Although the opportunistic lone-wolf fraudster still represents a threat, the industrialisation of fraud presents a far greater risk. With the advent of fraud farms and GenAI, the fraud prevention goalposts have shifted dramatically, as this nascent technology acts as a force multiplier and lowers the barriers to commit complex fraud.

From synthetic identities that evade traditional verification to deepfakes that subvert authentication, there is no doubt that the fraud landscape has changed forever.

As the scale and complexity of the fraud threat develops, businesses need to integrate fraud signals from multiple tools to mitigate it effectively. **Fragmented solutions that do not connect in an overall fraud score are no longer sufficient.**

The most advanced fraudsters know how to fly just under the radar of many fraud prevention thresholds by getting close but not exceeding fraud alert triggers. By combining different signals, businesses can connect the dots from multiple fraud data points for a more accurate overall decision.

This report features insights from a Forrester Consulting survey of 449 senior fraud leaders across eight countries – commissioned to understand the key challenges and opportunities in the current environment. We'll discuss why the adoption of ML-based, orchestrated fraud decisioning is no longer a choice, but a necessity for businesses to thrive in the coming years.

Experian is committed to making the digital world a safer place, and our global team of experts are constantly pushing to stay at the forefront of fraud detection and prevention technology. No matter what the size of your business, we can help you integrate the data and software you need to protect your business and customers.

We look forward to hearing from you and working together.

Problems

The industrialisation of fraud

Discover year-on-year increases in fraud attack types by industry. Explore the threat shift from individual fraudsters to commercial syndicates and the impact of GenAI.

Top fraud challenges and priorities

What are the top priorities and challenges in fraud prevention for the year ahead?

Solutions

Collaboration through data sharing

Joining forces is essential in the fight against fraud.

Connecting multiple fraud signals

Layering fraud signals is now essential, and integrating different fraud solutions is key to achieving this.

Key takeaways

Discover the biggest lessons from this year's research and focus areas to combat fraud for the year ahead.

Glossary and survey firmographics

Understand the terminology used in the report and the location, industry and role of the respondents.

SNAPSHOT OF KEY FINDINGS

73%

agree that GenAI has changed the fraud landscape forever

73%

believe fraud orchestration platforms are becoming essential to manage multiple fraud tools

71%

agree that AI/ML based fraud solutions are critical to stay at pace with a growing fraud threat

61%

find that false positives cost them more than fraud losses

59%

are struggling to find the right balance between security friction and good customer experience

55%

have seen an increase in overall fraud attacks in the past year

Base: 449 EMEA & APAC fraud decision-makers in Financial Services, Telcos and eCommerce
Source: Experian research conducted by Forrester Consulting August 2024

THE INDUSTRIALISATION OF FRAUD

Fraud trajectory continues upwards

Although the global macroeconomic situation is steadily improving, the fraud threat remains high. There are two key factors affecting this – geopolitical fragmentation and the impact of new technology. When these are combined with the persisting financial pressure many regions are still experiencing, the end result can only be described as a fraud inflexion point.

Our research shows that the fraud threat is undoubtedly growing, with 53% of Telcos and 57% of Financial Services seeing an increase in the volume of fraud versus the previous year. This trajectory shows no signs of slowing down either, with 57% of respondents expecting more fraud attacks in the upcoming 12 months compared with the previous year. A similar percentage (55%) expect their fraud losses to increase in the year ahead.

"We are facing an epidemic in the growth of financial fraud."

Jüren Stock
Secretary General
INTERPOL

Base: 449 EMEA & APAC fraud decision-makers in Financial Services, Telcos and eCommerce
Source: Experian research conducted by Forrester Consulting August 2024

YEAR-ON-YEAR INCREASE IN FRAUD ATTACK TYPES BY INDUSTRY

FINANCIAL SERVICES	TELCOS	ECOMMERCE
Saw an increase in overall fraud attacks		
57%	53%	43%
Expect fraud losses to increase in the next 12 months		
61%	48%	51%

Significantly increased | Increased

FINANCIAL SERVICES	Significantly increased	Increased		TELCOS	Significantly increased	Increased		ECOMMERCE	Significantly increased	Increased	
Identity theft fraud attacks	24%	33%	57%	Synthetic consumer identity fraud attacks	20%	40%	60%	Friendly fraud attacks	19%	26%	45%
Bot/credential-stuffing fraud attacks	21%	33%	54%	Money muling	28%	25%	53%	Identity theft attacks	22%	22%	44%
API fraud attacks	16%	38%	54%	Account takeover fraud attacks	27%	26%	53%	Refund fraud abuse	19%	24%	43%
Money muling	27%	25%	52%	Bot/credential-stuffing fraud attacks	25%	27%	52%	Account takeover attacks	17%	22%	39%
Synthetic business fraud attacks	21%	31%	52%	API fraud attacks	24%	28%	52%	Loyalty/reward fraud attacks	14%	24%	38%

Base: 449 EMEA & APAC fraud decision-makers in Financial Services, Telcos and eCommerce
Source: Experian research conducted by Forrester Consulting August 2024

The growing need to detect fake businesses

Synthetic business fraud attacks (52%) are increasing faster than synthetic consumer identity attacks (49%).

The **British government agency** that registers businesses adds around 4,000 companies each day – about 800 of these are fake. In the past, these were often used as shell companies, but they are increasingly being use to commit fraud through loans.

Base: 449 EMEA & APAC fraud decision-makers in Financial Services, Telcos and eCommerce
Source: Experian research conducted by Forrester Consulting August 2024

KYF – Know Your Fraudster

It is not just new technology that is impacting the fraud landscape. Over the past year, there have been several reports of highly organised criminal syndicates based in large office parks where tens of thousands of people have been coerced into conducting fraud at an industrial scale. By some reliable estimates, hundreds of thousands have been forced into online criminality in Southeast Asia alone.

The United Nations' latest fraud report discusses the increasing professionalisation of criminal operations and describes how cyber-enabled fraud operations have taken on industrial proportions. **They explain how fraud gangs have consolidated into large criminal syndicates, indicating a convergence of digital fraud, underground banking and transnational organised crime.**

Compounding this challenge is the advent of Generative AI (GenAI), which enables scams by providing engaging real-time conversation scripts in dozens of languages. Nearly three-quarters (74%) of our respondents believe the biggest fraud threat is social engineering scams, where consumers willingly hand over PII and payment data. There are a huge variety of social engineering scams, and when these are turbocharged by vast workforces and the force multiplier of GenAI technology, the scale of the threat becomes apparent.

HOW BAD IS THE SCAM THREAT?

According to one global consumer study 85% of respondents reported receiving a digital scam attempt in the last year.

NEXT LEVEL VISHING WITH FAKECALL

This malware tool is hidden in apps and hijacks phone calls to financial institutions – routing them to scammers instead. It also records all conversations, monitors screen activity and tracks your location to harvest PII.

BILLION-DOLLAR SCAM MARKETPLACES

Fraudsters can access thousands of tools and services through fraud superstores – including software, money laundering services and equipment to control fraud farm victims.

The impact of GenAI on fraud

The algorithmic arsenals that fraudsters now have at their fingertips have completely redefined the fraud threat. Nearly three-quarters (73%) of the fraud prevention professionals in our survey agree that GenAI has changed the fraud landscape forever. A similar number (69%) agree that public access to GenAI is increasing the fraud threat.

HOW EASY ARE SCAMS WITH GENAI?

Cornell University researchers wanted to know if they could create an autonomous AI scam agent – they were overwhelmed by how well it worked. It stole credentials 60% of the time in less than two minutes for under a dollar.

AROUND HALF OF BUSINESSES ARE ALREADY NOTICING THE IMPACT OF GENAI ON FRAUD

55% are seeing an increase in GenAI-influenced identity attacks

53% state that GenAI has had a noticeable impact on fraud losses

51% are seeing an increase in GenAI automated code bot attacks

50% are seeing an increase in GenAI-influenced APP attacks

Put simply, there are now more tools available for fraudsters to commit sophisticated fraud, with much less effort required. An example of this is fake identity generation. The website OnlyFake.org – which is one of hundreds of similar services – gained a lot of attention by producing highly realistic fake passports and driver's licences that can pass basic authentication checks for only $15. They claimed to be producing 20,000 a day!

Perhaps the most telling finding from our research about this topic is that more than half of respondents (56%) struggle to identify if GenAI has been involved in a fraud attack, and therefore find it difficult to quantify the impact of GenAI on their fraud losses.

PREVENTING GENAI-POWERED FRAUD

Each fraud solution has a distinct approach to identifying fraud – when these are combined into an overall recommendation the resulting decision is much stronger than the sum of its parts.

Base: 449 EMEA & APAC fraud decision-makers in Financial Services, Telcos and eCommerce
Source: Experian research conducted by Forrester Consulting August 2024

Nearly two-thirds agree their organisation should invest more in the latest technology to better protect customers.

Who is responsible for fraud prevention?

As the technology used to prevent fraud has progressed, fraudsters are increasingly targeting the weakest link – people. Scams allow fraudsters to circumvent most fraud controls as their victims unwittingly unlock access to their accounts or share data. And to facilitate this, fraudsters depend heavily on social media.

A huge variety of Authorised Push Payment (APP) fraud and money mule recruitment originates via social media channels. While some jurisdictions are moving to regulate these platforms, they are currently shielded from any liability for the content their users' post. However, the role of social media in the rise of fraud should not be underestimated and urgently needs to be addressed.

When it comes to fraud loss liability, the UK's recent PSR and CRM legislation is leading the way, requiring mandatory APP fraud reimbursement and splitting costs 50/50 between sending and receiving institutions. In comparison, the EU's PSD3 only concedes liability for bank impersonation scams, which still leaves a lot of room to improve the duty of care responsibility that financial institutions bear.

According to our research, 63% of respondents believe the fraud liability shift for APP fraud creates a stronger incentive for financial institutions to invest in improved security measures and fraud detection systems.

BALANCING FRAUD PREVENTION RESPONSIBILITY

63% believe the fraud liability shift for APP fraud creates a stronger incentive for financial institutions to invest in improved security measures.

52% feel that financial institutions are being forced to provide policing services as law enforcement is struggling to contain the growing impact of fraud.

However, more than half (52%) feel that financial institutions are being forced to provide policing services as law enforcement is struggling to contain the growing impact of fraud. 56% of the fraud professionals in our survey agree that central banks should prevent financial institutions from opening new accounts and issuing credit cards if their fraud prevention controls fall below an acceptable standard.

As the liability debate continues, with considerable differences between legal requirements across the globe, the key question remains: Who is ultimately responsible for digital fraud prevention?

Base: 449 EMEA & APAC fraud decision-makers in Financial Services, Telcos and eCommerce
Source: Experian research conducted by Forrester Consulting August 2024

TOP FRAUD CHALLENGES AND PRIORITIES

Machine Learning as the backbone of fraud prevention

Introducing ML-based fraud models is the top fraud priority for the year ahead. This is unsurprising, considering the increasing fraud threat and the critical role this technology plays across a range of essential fraud tools, and in the decisioning process that determines the final outcome.

However, in the battle of good AI versus bad AI, it's important to understand that the type of ML model and the data used to train it make a fundamental difference in effectiveness. **Simply using ML does not necessarily guarantee an improvement in fraud prevention.**

Although many businesses are starting to recognise the need for ML, more than half (53%) are struggling to implement it. Why is that? Our research suggests that access to sufficient training data remains a stumbling block, with a similar number (54%) stating that they lack quality data.

Developing effective ML models in-house is a significant challenge when compared to using verified, pre-trained models and established frameworks. Off-the-shelf ML models can be customised and adapted to specific organisational needs, which accelerates time to deployment and time to value.

This is where external partners can play a critical role. Close to four out of five recognise this, with 78% agreeing that collaboration with external partners is crucial for effective fraud prevention.

Base: 449 EMEA & APAC fraud decision-makers in Financial Services, Telcos and eCommerce
Source: Experian research conducted by Forrester Consulting August 2024

Base: 449 EMEA & APAC fraud decision-makers in Financial Services, Telcos and eCommerce
Source: Experian research conducted by Forrester Consulting August 2024

Reduce investigation costs with fewer manual reviews

Alongside the introduction of ML, reducing investigation costs is an equally important priority for fraud leaders. Fortunately, these priorities work together, as ML can help to automate more fraud decisions – which reduces the effort and cost associated with manual reviews.

The improved accuracy of ML-based fraud detection can also directly address the fourth and fifth fraud priorities, minimising fraud losses and reducing false positives. A staggering 61% of respondents report that false positives cost them more than fraud losses. High numbers of false positives impacting revenue goals was also highlighted as the second biggest challenge associated with fraud prevention.

Agility in adjusting models, rules and scores is a key challenge

When we compare the top fraud priorities against the biggest challenges limiting fraud prevention, we see some common themes. The ability to rapidly update models, rules and scores is critical for businesses to stay agile in the face of a highly dynamic fraud threat. Traditional rules-only fraud controls require experts to manually identify the latest fraud signals and build new rules.

ML analysis of fraud attacks can uncover new patterns, which can help with the development of new rules to keep businesses at pace with changing fraud attack vectors. When first introduced, ML models can run silently in the background alongside a traditional rules engine to build confidence in the benefits of this approach.

Biometrics and device data as critical fraud prevention layers

As fake and synthetic IDs become harder to detect, more businesses are recognising the need for additional fraud signals – particularly selfie liveness detection and device profiling. Nearly two-thirds (63%) of respondents agree that device profiling is a must-have component of any fraud strategy.

Without liveness detection, digital authentication is increasingly at risk due to the advancements in GenAI-produced deepfakes. **Only AI is capable of differentiating between deepfakes and real people,** as the flaws in deepfakes are now often unnoticeable to the human eye.

Base: 449 EMEA & APAC fraud decision-makers in Financial Services, Telcos and eCommerce
Source: Experian research conducted by Forrester Consulting August 2024

agree that combining fraud and AML has increased operational efficiency and improved risk management

FRAML - Integrating AML and fraud prevention

The merging of fraud prevention and Anti Money Laundering (AML) is growing momentum as more businesses see the value of integrating these traditionally separate departments. Including real-time PEPs and sanctions checks as part of identity and fraud screening during onboarding can provide a more holistic view of the customer.

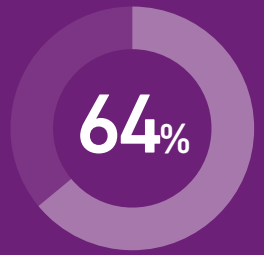
The benefits of a unified FRAML approach are reflected in our research, with nearly two-thirds (65%) agreeing that combining fraud and AML departments has increased their operational efficiency and improved risk management. However, many businesses (60%) still perceive AML as a compliance risk rather than a security risk.

Optimising FRAML requires an orchestration platform that can automate the process of scanning the latest consolidated global watchlists and then seamlessly integrate this data with existing identity and fraud checks. This automated approach allows for better customer service by reducing delays, while still maintaining the highest levels of AML compliance.

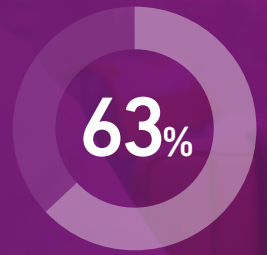
CONSORTIA: COLLABORATION THROUGH DATA SHARING

A fraud consortium is a strategic alliance of institutions and service providers united in the common goal of comprehensively understanding and combatting fraud.

BENEFITS



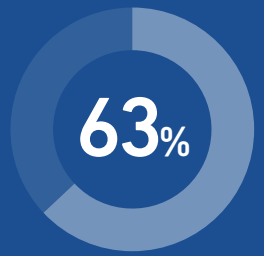
have seen positive ROI from investing in a fraud consortium



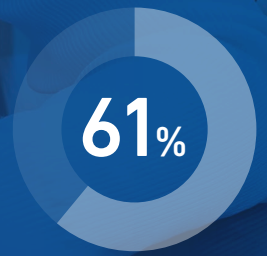
agree that sharing fraud data with others through a consortium is an effective way to identify new and emerging fraud trends

believe fraud consortia will play an increasingly important role in fraud prevention efforts in the next five years

CHALLENGES



feel that fraud consortia need to improve their ability to share data securely and efficiently across different industries



state that privacy regulations in the country/countries their organisation operates in make it difficult to share valuable fraud data in a consortium

believe there is a lack of clear standards for data governance and security within many fraud consortia

Base: 449 EMEA & APAC fraud decision-makers in Financial Services, Telcos and eCommerce
Source: Experian research conducted by Forrester Consulting August 2024

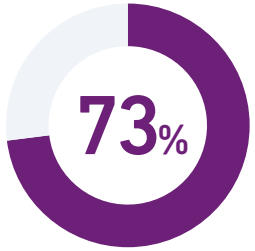
CONNECTING MULTIPLE FRAUD SIGNALS

Our research shows that behavioural biometrics, shared consortium data and integrating AML with fraud decisioning are the top areas for investment in the next 12 months. Although these capabilities are increasingly important, they do introduce additional challenges – particularly around the complexity involved with integrating multiple fraud signals and solutions into a single decision.

More than three-quarters (76%) of businesses use multiple fraud solutions from different vendors, and stitching these signals together presents a real challenge. **Without connecting different fraud signals into a single decision, businesses are putting themselves at a disadvantage.** More than half (58%) of respondents stated that their fraud prevention solutions do not work synchronously.

It's important to consider that no individual fraud solution is capable of detecting fraud 100% of the time – which means the most effective fraud strategy involves multiple layers of fraud checks. **But as important as having multiple layers of fraud signals is the ability to integrate the scores from various tools.**

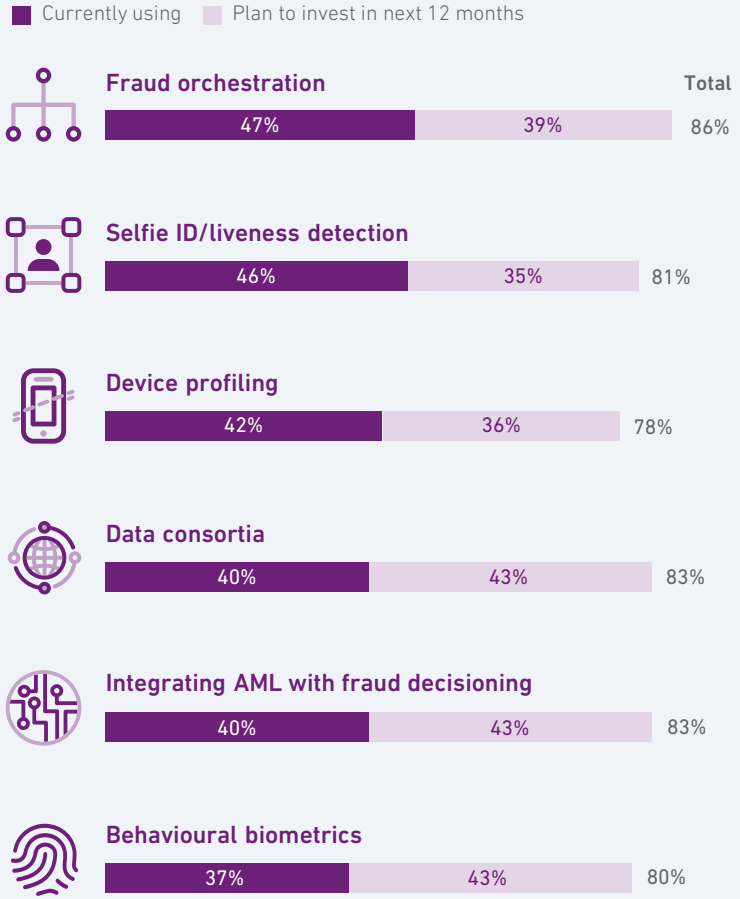
Using a single platform to orchestrate multiple fraud tools and integrate their outputs into one decision significantly enhances the accuracy of fraud prevention.



agree that fraud orchestration platforms are becoming essential to manage multiple fraud tools

Base: 449 EMEA & APAC fraud decision-makers in Financial Services, Telcos and eCommerce
Source: Experian research conducted by Forrester Consulting August 2024

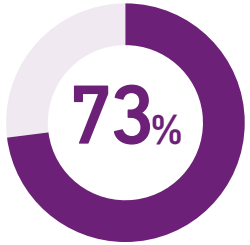
CURRENT AND FUTURE FRAUD CAPABILITY ADOPTION



How can orchestration improve customer experience?

Balancing strong fraud controls with a smooth user journey is an ongoing challenge, with 59% struggling to find the right balance between security friction and good customer experience. More than half of respondents (52%) state that they prioritise security, even if that introduces friction. However, with the right orchestration platform, it is possible to have your fraud prevention layer cake and eat it.

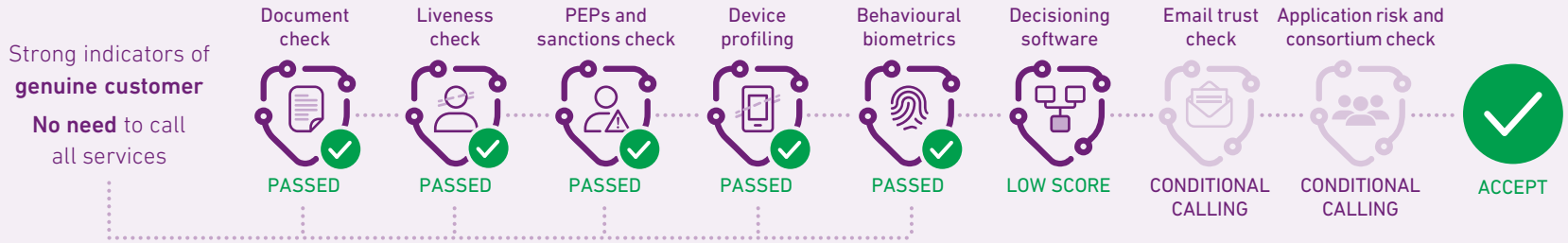
While orchestration can significantly improve fraud detection, it plays an equally important role in enhancing customer experience. Instead of every new or returning customer facing the same level of friction, it allows for relevant fraud checks to be dynamically called – depending on the customer's risk threat.



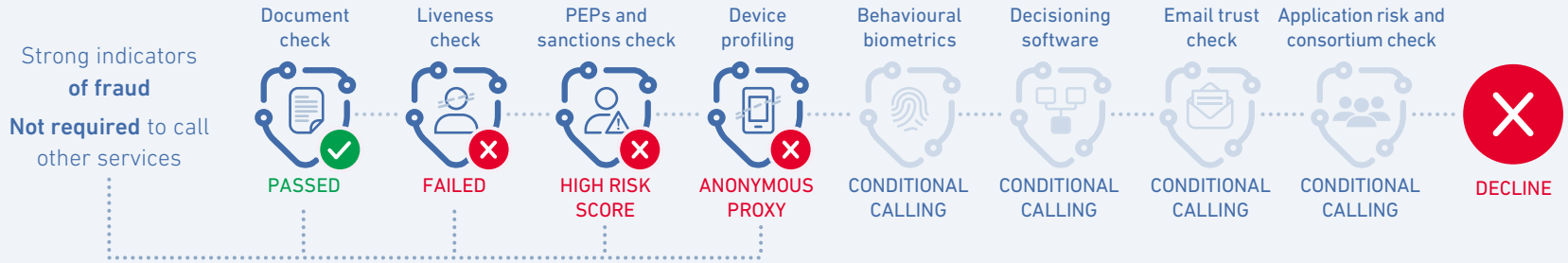
agree that orchestration of fraud signals is critical to reduce onboarding friction

Fraud services can be called simultaneously to reduce response time. Connected via flexible API, multiple services can work in a coherent way - reducing friction and costs.

SCENARIO ONE



SCENARIO TWO



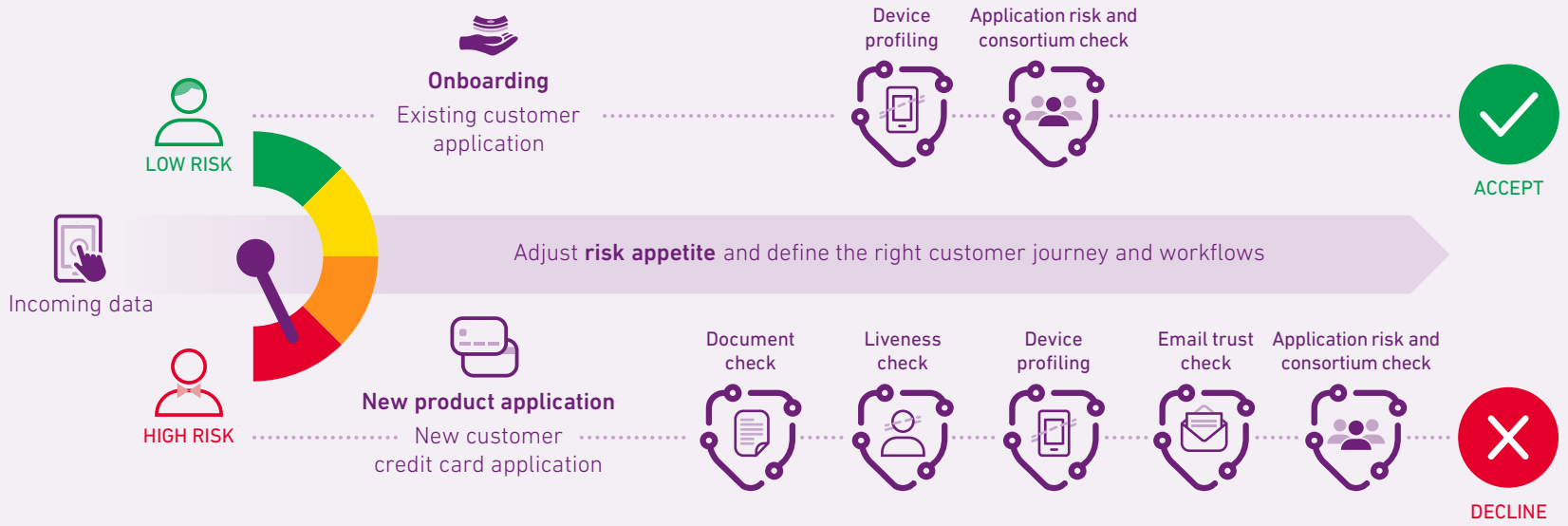
Using predefined customer workflow journeys means that low-risk customers experience zero friction with passive checks – such as device profiling and behavioural biometrics – happening in the background. For a customer who has failed the initial device checks, a series of additional checks can be called in parallel or one after the other.

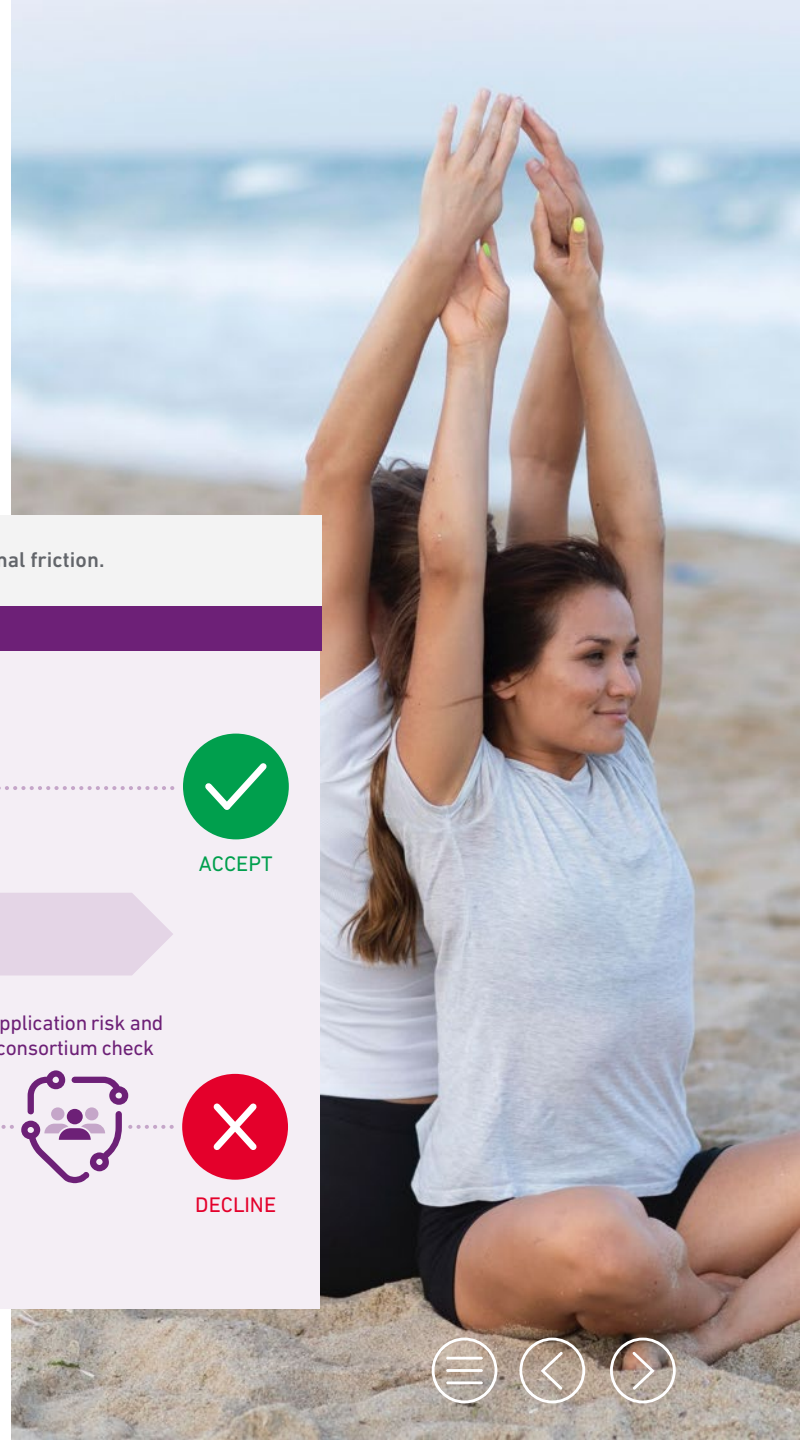
This means that good customers have a fast and simple application or checkout journey, while suspect customers have to complete additional steps to verify their bona fides. Nearly two-thirds (64%) of respondents agree that selecting appropriate fraud checks based on individual customer risk is the future of fraud prevention.

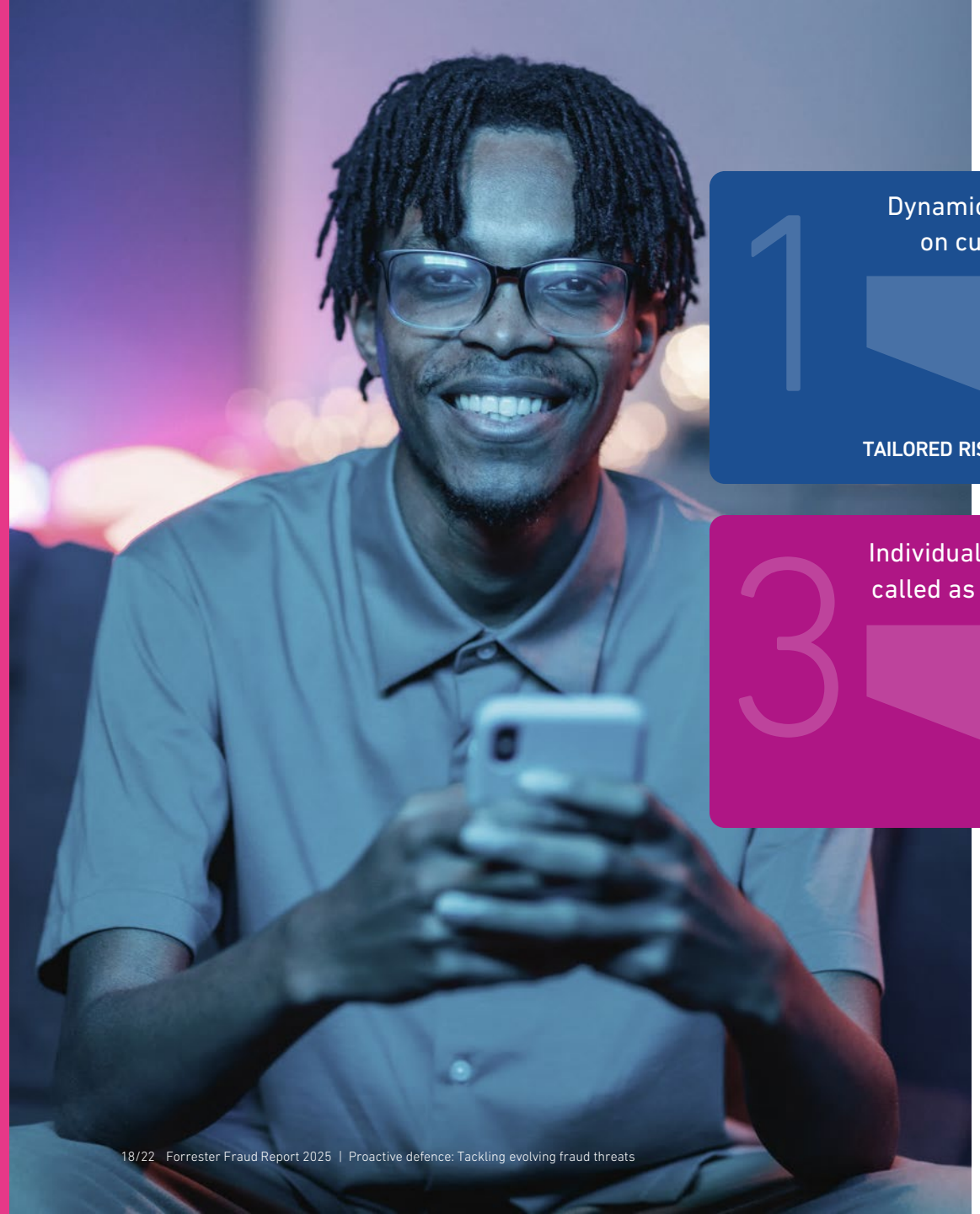
BALANCING RISK AND FRICTION

Depending on the risk level of the consumer, calling additional services may be required. However, low-risk customers pass through with minimal friction.

HOW IT WORKS







Main benefits of accurate orchestration and decisioning

1 Dynamic fraud checks based on customer risk score

TAILORED RISK-BASED FRAUD DETECTION

2 Improved experience with less friction for good customers

IMPROVED USER EXPERIENCE

3 Individual fraud checks are only called as required by the threat

REDUCED COST

4 Greater precision in identifying good versus bad customers

FEWER FALSE POSITIVES

With 66% of businesses planning to increase the number of fraud solutions they use in the next 12 months, it's clear that orchestration has a critical role to play in managing multiple fraud signals. For those businesses already using orchestration, 72% state that it has helped them reduce false positives, and 69% believe it has increased their operational efficiency.

KEY TAKEAWAYS

Fraud losses are increasing

More than half of businesses have seen an increase in fraud losses over the past year, with 55% expecting their fraud losses to increase further over the next 12 months. As fraud becomes more commercialised and entrenched in global organised crime, 59% admit to struggling to keep up with this rapidly evolving threat.

GenAI has fundamentally changed fraud

GenAI is rapidly transforming the way fraudsters operate. Close to three-quarters (73%) of fraud prevention professionals agree that GenAI has changed the fraud landscape forever. Considering how new this technology is, it's fair to say that we have only seen the tip of the iceberg when it comes to GenAI-powered fraud.

Orchestration and ML are key to managing fraud

Including multiple fraud solutions is critical to mitigating fraud, yet connecting these different fraud signals is equally important. A fraud orchestration platform allows for individual services to be dynamically called based on the risk level – this improves fraud detection accuracy, reduces costs, and enhances customer experience.

GLOSSARY AND SURVEY FIRMOGRAPHICS

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 and 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 biometric 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.

Injection attacks
A cyber-attack where a deepfake is inserted directly into the data stream powering an identity check.

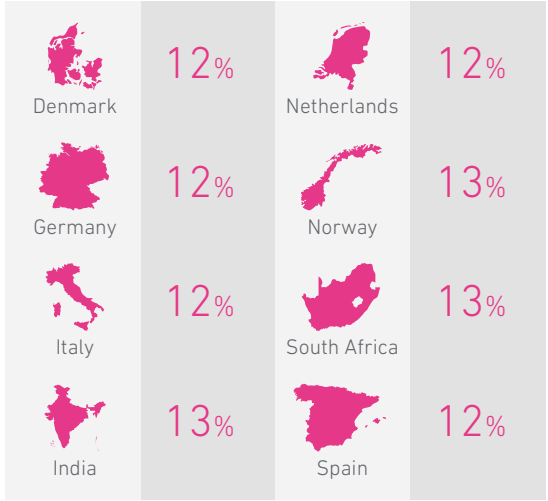
Money muling
A person who helps launder criminal gains by receiving money into their account and then transferring it into another account on behalf of a fraudster. These middlemen are often recruited on social media and may be unaware that money muling is illegal.

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

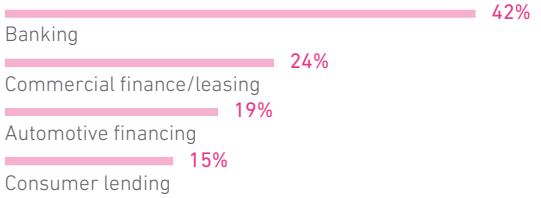
Synthetic identity
A combination of real and fake PII data is used to create a difficult-to-detect fabricated identity.

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.

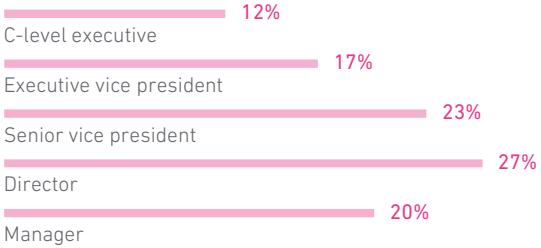
RESPONDENTS BY COUNTRY



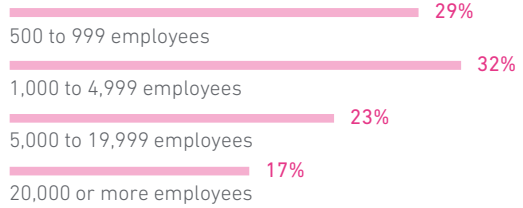
FINANCIAL SERVICES BY SECTOR



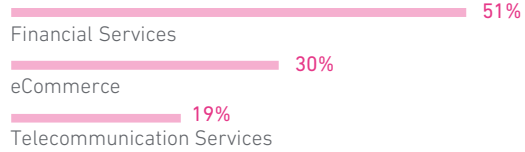
POSITION OF RESPONDENT



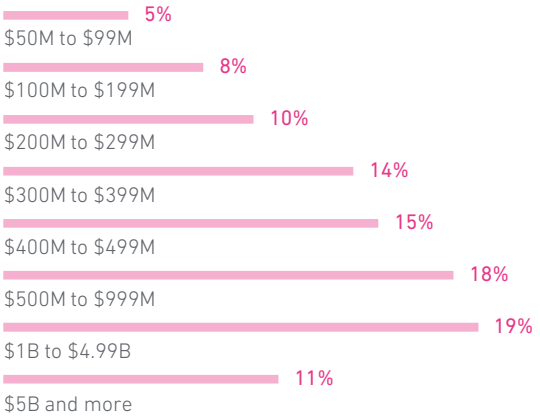
EMPLOYEE SIZE



INDUSTRY



ANNUAL REVENUE



ABOUT EXPERIAN

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

We help redefine lending practices, uncover and prevent fraud, simplify healthcare, deliver 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, agribusiness, insurance, and many more industry segments.

We invested in talented people and new advanced technologies to unlock the power of data and innovate. As a FTSE 100 Index company listed on the London Stock Exchange (EXPN), we have a team of 22,500 people across 32 countries. Our corporate headquarters are in Dublin, Ireland.

Learn more at experianplc.com

Over 1,700 businesses rely on Experian's fraud detection, identity verification, and authentication solutions, saving $12 billion in fraud losses annually. With our end-to-end solutions you can strengthen governance, streamline customer experience and boost growth by confidently approving more applications.

Find out 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