# **Preventing fraud** in challenging times

## EMEA FRAUD REPORT 2020

experian™

# Index

# Introduction

This year, more than any in recent history, has highlighted just how adaptable, unrelenting, indiscriminate and opportunistic, fraudsters are.

While the global pandemic, subsequent social and commercial lockdowns have posed huge unpredictable challenges for us all, fraud has continued unabated - especially via digital channels where many consumers' day-to-day business is now being transacted.

While the criminals have quickly adapted - often faster than legitimate customers - it's clear as highlighted in last year's report there are still significant gaps in many firms' abilities to react and meet the challenges head-on. Inside, we take a deep dive into emerging trends, highlight where business is exposed and where many admit they're hampered by the sheer scale, complexity and diverse methods now being adopted by fraudsters.

Despite typical challenges of budgets, know-how, talent, recruitment and staff retention, the pandemic has rewritten the rules and will continue to have an impact for some time to come.

# ABOUT THE AUTHOR

**Frédéric Dubout**

Senior Consultant in Fraud and Identity Experian

Frédéric has 20 years' sector-specific expertise working for multi-national telecommunications, banking, automotive and financial services companies, across Europe, Africa and the Middle East. Frédéric has worked across the full spectrum of fraud prevention - from the application of emerging technologies and biometrics, to transactional and payments fraud, to application fraud, online, mobile and card-not-present fraud. Collections, data quality, data management and project management, also fall under his areas of expertise.

## METHODOLOGY

During the summer of 2020, we received direct insight from more than 150 senior decision-makers with responsibility or influence over fraud and risk strategy at businesses across Europe, the Middle East and Africa (EMEA).

# Exec Summary

- The majority (89.2%) of respondents believe fraud management is a high priority within their company.
- But take a deep dive into operational aspects and confidence in overall performance drops significantly to around 60%.
- In fact, nearly two in five (37.5%) firms don't believe they successfully tackle fraud across all channels.
- More than a third (36.7%) also have low confidence in their fraud metrics.
- Fraudsters have been quick to adapt and exploit the pandemic with around two in five (37.7 %) respondents noting a spike in three fraud types – all related to digital channels.
- They are Sim-swapping, phishing-related scams and account takeover frauds.
- Respondents all reported increases in alert rates, frequency of attacks and a rise in residual fraud rates.
- During the pandemic, business continuity was front-of-mind for almost one in six (16%).
- Nearly half (42.6%) of survey respondents believe their fraud prevention resources are insufficient.
- In fact, the majority (54.5%) blame increasingly complex fraud types.
- Nearly half (49.1%) of all respondents also admit they need to adopt a more balanced approach to fraud prevention.
- But it's also proving challenging when referral capacity is constrained by resources - particularly if fraud attacks rates are on the rise - because it's unlikely risk appetites can be changed overnight.
- Around one in three (30.3%) say the volume of fraud has increased faster than headcount.
- More than half (51.2%) say they are not able to handle emerging fraud threats.
- Of these, around one in 13 (7.5%) is already struggling to cover current fraud threats with existing resources.
- Improvements to rules engines and real-time analysis of transactions was key for more than half (50.9%).
- But aspirational investment in device intelligence, email verification, AI, machine learning and greater automation are likely to be priorities for around one in five fraud teams.

# Market context

From the outset, we were keen to assess opinion relating to confidence and trust in the overall effectiveness of fraud systems. Participants were asked for their opinions on performance in detecting and preventing fraud within their firms. A snapshot of key results is below.


The majority 89.2% believe fraud management is a high priority within their company.


But more than a third (36.7%) say fraud metrics are not standardised or regularly measured within their organisation.


In fact, nearly two in five (37.5%) firms don't believe they successfully tackle fraud across all channels.

It's clear confidence has two sides. Generally, it's quite high among the vast majority of respondents. But take a deep dive into operational aspects and confidence in overall performance drops significantly to around 60%. There's clearly room for improvement given 36.7% have low confidence in their fraud metrics, while a similar number (37.5%) admit they can't tackle fraud across all channels.

## Regional variances

Half (50%) of respondents in South Africa believe that the proposed approaches to fraud prevention within their market are too expensive, highlighting a clear need for a tailored and scalable capabilities.

## REGIONAL VARIANCES IN RESPONSIBILITY FOR FRAUD MANAGEMENT

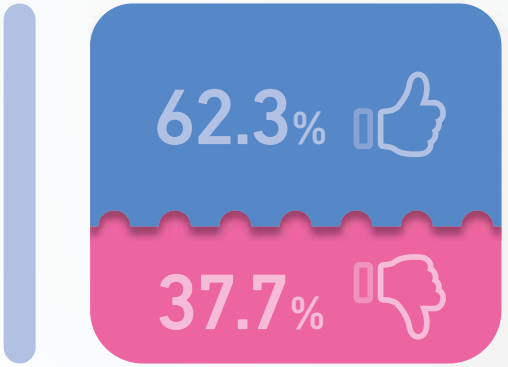
Across EMEA, most fraud teams are aligned with in-house risk departments.

But there are some notable regional exceptions. In Turkey and South Africa, firms generally favour including their fraud teams within operations, while finance if preferred in France. In Denmark, fraud has a clear and well-defined focus within commercial legal and compliance divisions.

# Challenges and emerging trends

## EMERGENCE OF NEW OR VARIED FRAUD TYPES WITHIN THE PAST YEAR

Fraudsters have been quick to adapt and exploit the pandemic with 37.7% of respondents noting a spike in three fraud types – unsurprisingly all related to greater reliance on digital channels, particularly among less savvy customers.




1*

### Sim Swap

Cyber-criminals hijack cell phone numbers to gain access to sensitive personal data and accounts.

2*

### Phishing-related scams

Fraudsters attempt to steal sensitive data and personal information including usernames, passwords and credit card details, by disguising themselves as a legitimate, trustworthy entity in an electronic communication.

3*

### Account Takeover

When thieves use a legitimate customer's details to take control of their online accounts to steal money or make illegal credit card purchases. None of these fraud trends are new, but they're all on the rise and they are directly linked to our increased reliance on digital interactions.

## SIM-SWAP FRAUD IS BACK WITH A VENGEANCE

Among the notable fraud trends to emerge across the region this year is the prevalence of so-called Sim-swapping. It's not a new technique – it's been around for as long as high-performance web-enabled mobile devices have. But feedback from our survey participants confirms high volume, old-school Sim-swapping hijacks, in line with other digital frauds, are back with a vengeance – and clearly, it's an area that deserves greater scrutiny.

On the face of it, Sim-swapping is a legitimate and useful way to switch mobile device, update damaged, lost or stolen cards while retaining existing phone numbers. Historically, this type of fraud was adopted simply to direct traffic to premium-rate numbers, clock-up inflated roaming charges and so on, to derive income. But with digitisation, there's been a more general drift and preference for authentication using OTP (one-time passwords) via SMS text messages to prove the 'possession' part of any two-factor authentication. But the objective of these types of frauds quickly shifted to the theft of financial assets, mainly by getting access to online bank accounts, before emptying them by making transfers to other controlled accounts - either directly or indirectly via mules.

Clearly, stealing cash directly is far more appealing and efficient than being obliged to monetise premium rate telephone calls. PSD2 is also set to render the OTP / SMS process obsolete as a payment authentication method. Instead, strong customer authentication (SCA) is promoted through stricter methods that use the combined factors of possession, inheritance and knowledge.

## WHAT MAKES SIM-SWAP FRAUD POSSIBLE?

There's no single definitive answer. But instead, a combination of factors has evolved to contribute to its prevalence.

First, the choice by companies to readily adopt SMS as the go-to factor of 'possession' in the two-factor authentication of their customers. At the same time, background processes have historically been poorly secured by operators – they're often vulnerable to social engineering and identity theft – particularly in call centres. Second, there's a lack of traceability and accountability of Sim cards, with poor controls in the supply chain.

The advent of eSIM is likely to only make a modest dent in the scale of the challenge - phone numbers can still be transferred from one phone to another, via a dedicated process, which must in turn be properly secured.

Finally, as with most frauds, the constant weak line is the customer, who continues to be vulnerable to social engineering. It's a challenge that extends far beyond Sim-swap given it's one of many digital frauds devised to seamlessly sidestep authentication - especially two-factor methods.

> There are some notable regional variations in fraud trends. Spanish respondents uniformly noted a spike in Sim-swap fraud. But in Germany, where the majority of survey respondents (**58%**) were from banking and insurance, it was clear phising and man-in-the-middle attacks were regarded as far more prevalent than Sim-swaps.

As it stands, there are many alternatives to Sim-swap fraud besides the fraudulent switching of physical Sim cards or eSIMs. These include so-called MitMo malware – man-in-the-mobile, or man-in-the-browser frauds.

Elsewhere, hacks to signalling system 7 (SS7) - the protocols that enable the exchange of information between telephone networks - are also prevalent. SS7 hacks enable fraudsters to read text messages, listen to phone calls and track mobile users' locations with just the knowledge of their phone number. It also highlights a vulnerability in the infrastructure of the global mobile phone network. But given it's a targeted, selective and relatively labour-intensive route to fraud it's unlikely to be used on a large scale.

Malware also continues to be prevalent. These include so-called Muraena and Necrobrowser attacks. Both are similar, in that they're near-invisible routes to automating phishing and post-phishing activities.

## ROUTES TO EFFECTIVE RESPONSES

The threat posed from multi-layered fraud techniques requires an appropriate combination of detection and defence layers. There are also several tactical, albeit choppy steps, that can be taken to help prevent losses. These could include delaying transactions by up to 72-hours before completing a transfer, which offers a chance to act when suspicious activity is flagged up. Alternatively, transactions could be restricted to a limited number of well-known, well-identified and well-protected channels. Online eligibility checks of both identity, habit and behaviour – particularly following the loss, theft, or change of a mobile or card – is another possible option.

Point of sale controls with mandatory validation checks of old Sim cards, or the customer's identity, along with analysis of the cards' age, would also be effective. Similarly, checks to ensure geolocation consistency are also critical, given a phone simply cannot be 500kms to 2,000kms apart within a matter of minutes.

Of course, for vendors there's a trade-off because most of these solutions interfere with the customer experience - but none should be regarded as the exclusive responsibility of the telecom operators.

As noted, Sim-swap is just one fraud technique among several others that has jumped in prevalence thanks to our increased reliance on digital channels. This year's pandemic has also increased our all-round reliance on online routes. But clearly, when there are numerous vulnerabilities and multiple risk-factors, a systematic approach is required to detect, prevent and continually address the risk.

# PHISHING AND WAYS TO PREVENT CUSTOMERS FROM TAKING THE BAIT

Phishers prey on hard-won customer relationships. The biggest phishing attacks hinge on commercial email compromises. Phishers send emails that look familiar with a message that urges customers to complete a legitimate-looking online transaction that may include anything from updating an account, to selecting a loyalty discount, to a personalised special offer.

Customers react because they want to be helpful and are generally supportive of firms they trust – which is why these types of scams continue to work. But phishing emails are just the start. Fraudsters have moved beyond the blanket circulation of lottery scams and emails from anonymous African princes. Nowadays, attacks are personalised to both the business and a specific customer – with phishers often able to take advantage of automation and targeting tools, so they can get the most reward for their efforts.

Take for example a variation called 'spear phishing.' It's a scam that targets individuals with access to an organisation's financial accounts or internal systems. Another type known as 'whaling', will target a specific high-value individual simply because they have more money and are deemed a more lucrative opportunity. There's also so-called 'smishing', which is again a phish circulated to customers via text message.

Legitimate businesses are not the only ones using machine learning and artificial intelligence (AI) to grow - phishers are cashing in on it as well. Using compromised personal data is just the first step. Phishers then turn to machine learning and AI to compile detailed profiles of individuals including buying preferences, career, family, social profile and so on. The information is used to create a tailored, highly personalised message that is more likely to prompt the intended victim to act.

Phishing attacks will always be around, but there are steps that businesses can take to help safeguard their customers right now to stem the tide. The key is to focus on technology and training. Even small businesses can take advantage of available email blocking or filtering technology. Train employees to think twice when they receive an odd request before reacting to it. But most of all, continue to keep staff training updated – because the phishers never stop and are always evolving new routes to defraud.

## ACCOUNT TAKE OVER FRAUD

As with phishing, consumers' log-in details are often acquired following a wholesale data breach. Fraudsters use the stolen credentials to test account access and observe activity to understand the ebbs and flows of normal cash movement – by peering into private financial records – and verifying the optimal time to strike for the most financial gain.

Surveillance and fraud staging are seemingly transparent account activities that fraudsters undertake after an account has been compromised, but before the compromise has been detected or money is moved. Activities include viewing balances, changing settings to more effectively cover tracks and setting up account links to help pave the way and stage eventual fraudulent transfers.

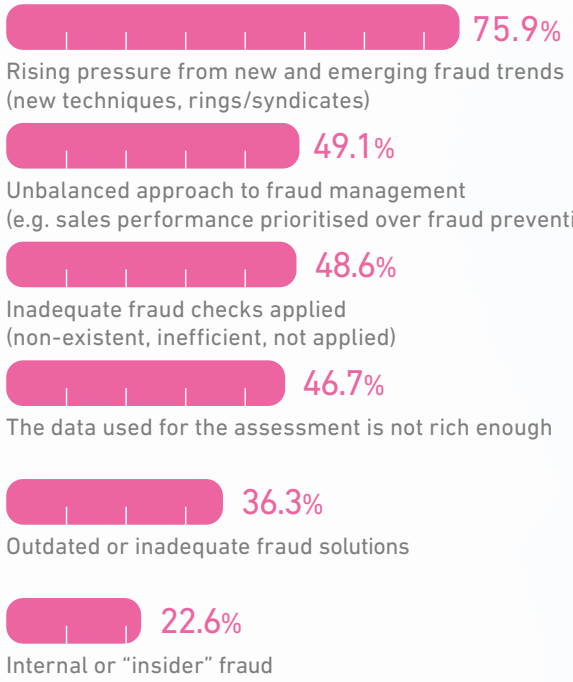
The unfortunate aspect is that the actual loss is often the final step that culminates from a series of fraudulent activities that simply weren't detected in time. It's an outcome that can severely undermine long-term consumer trust and can devastate a brand's reputation.

Heavy-handed security creates friction. It may well detect suspicious or unusual activity, but it can also be hugely frustrating for customers. Fraudsters are increasingly targeting loyalty schemes where they use acquired account data to log into reward programmes to either use a customer's acquired points to make a direct purchase or sell on the stolen points elsewhere at a discount.

Generally, loyal customers are the most attractive to fraudsters because they have the highest balances. But they're also very valuable to the business because they make regular and repeat purchases. They're not the sort of customers any firm wants to lose, but concerns over either lax or heavy-handed security, may simply push them into the arms of a competitor.

Success hinges on sophisticated account surveillance tools which can detect when a customer's online session is being used by multiple devices. The ability to detect replays of previous online sessions is also crucial, as is the ability to monitor multiple touch points across the customer lifecycle. Monitoring should include log-ins, habitual financial and non-financial transactions, which help builds up a behavioural profile that can later be used to detect malice and block suspicious activity.

# Why frauds are succeeding



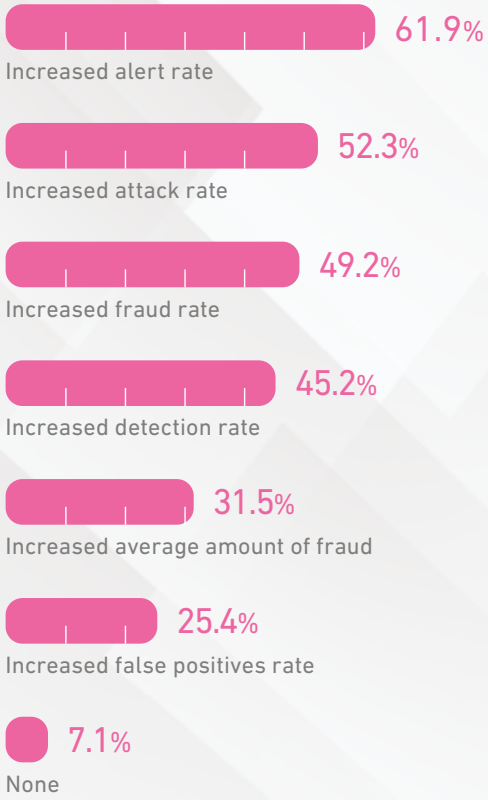

Two key points emerged around fraud types during this year's research. The increased complexity of fraud is the main reason why attempts succeed. At the same time, the effectiveness in dealing with suspicious activity directly hinges on a firm's resourcing, processes and capabilities.

Three-quarters of participants accept they need to be able to recognise and tackle increased, or evolving fraud trends. It's particularly vital that as new fraud rings emerge, organisations can identify links across all channels, often between seemingly unconnected activities and behaviours.

Around half of respondents (49.1%), also admit there's a need to ensure a balanced approach to detecting and preventing fraud. AI underpinned with machine learning techniques helps firms achieve a win-win, with increased fraud detection helping safeguard customers and increased revenues by reducing referrals and friction.

The ability to maximise and make the most of available data is also vital for nearly half (46.7%) of all respondents. Analysis through covert device intelligence is proving hugely successful in preventing suspicious transactions, while keeping online customer journeys friction-free.

# The pandemic's impact on fraud analysis and metrics



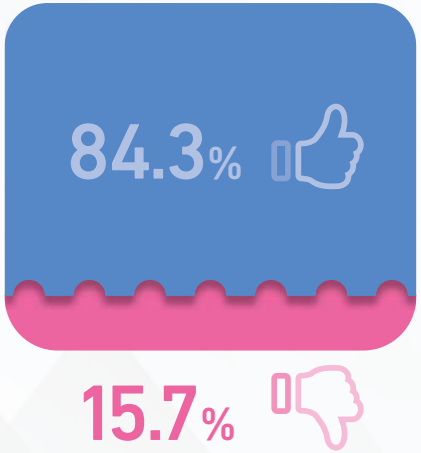

Survey respondents acknowledged a reported increase in alert rates, frequency of attack rates and a rise in residual fraud rates - when the overall number of transactions is used as the denominator.

The impact of lockdown on consumer demand has been clear. It prompted a sharp fall in commercial activity, before being subsequently punctuated by a broad switch to digital channels. As pandemic-related restrictions were eased, a gradual return to more 'traditional' channels has been noted.

But business had a far more marked sense of urgency. Decision-makers quickly realised the need to adapt fast to survive and migrate as many back-office activities as possible to remote and online working. There were inevitable casualties. Some firms were flexible and thrived, while others struggled and found it difficult, or even impossible.

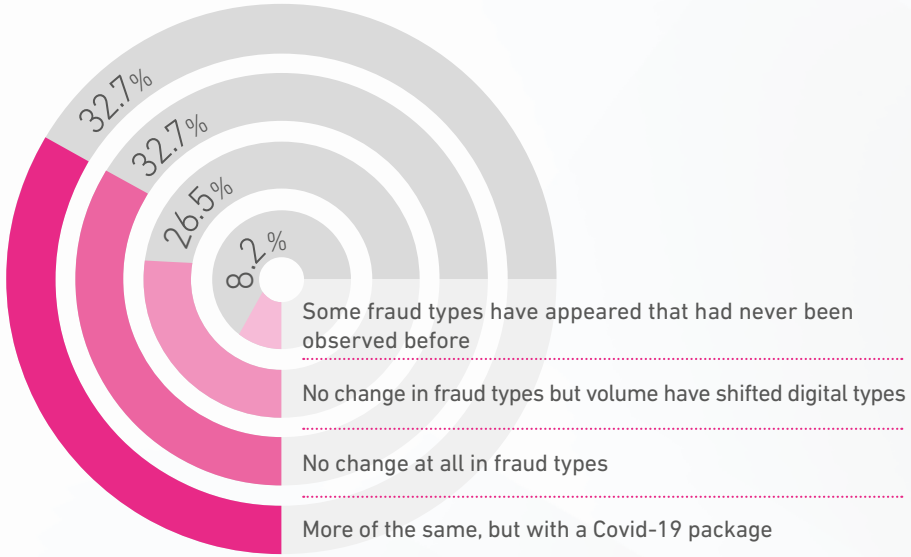
Business continuity was front-of-mind for many. In fact, fraud managers' main fears hinged on an acute loss of efficiency that risked undermining their ability to prevent, detect and process fraud as quickly and accurately as before. According to the survey findings, it was a concern that was justified for almost one in six (16%) participating companies. Among some firms it prompted a complete re-think about their long-term organisation, structure, tools and future reliance on automation – particularly during the pandemic's second wave, or in helping mitigate any subsequent surges.

Did **business continuity** issues **enable some frauds** to succeed where they would have failed before?



## FRAUD TYPES NOTED AT THE HEIGHT OF THE PANDEMIC

Around one in 12 firms saw new trends emerging at the height of the pandemic's first wave, while another one in three also saw an uptick in attempts directly linked to the outbreak.




## EMERGING TRENDS

Unsurprisingly, nearly all fraud teams intuitively knew the chaos and societal uncertainty the pandemic delivered would drive opportunist frauds. It's a point also borne out by the survey's findings. Respondents readily admit fraudsters' relentlessly adaptable attacks were evident from the outset as they stepped up the rate, frequency and variety of attempts, which in normal circumstances would be far easier to detect and thwart.

Various types of social engineering – notably phishing - were among the most prevalent forms of attempted fraud. Spoof emails and texts were presented as official messages from authorities, institutions or companies. The approach directly preyed on heightened levels of anxiety in a bid to trip up less digital-savvy consumers, when many were obliged to switch to far less familiar online channels during lengthy periods of lockdown.

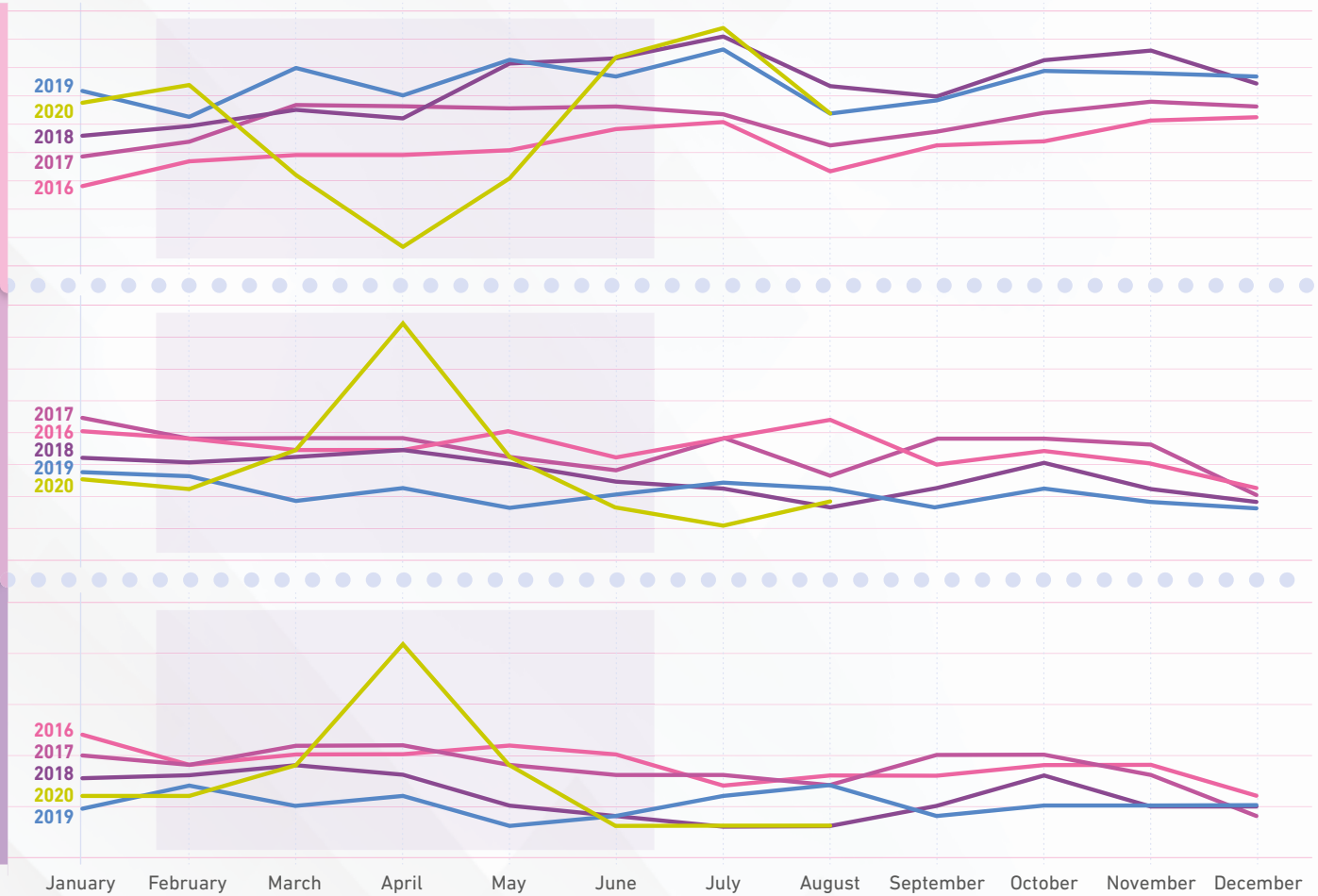
Analysis among a set of EMEA clients involved in one of our regional collaborative fraud data sharing schemes shows year-on-year patterns between applications volumes, attack rates and fraud rates. The comparison also demonstrates just how relentless fraudsters were at the height of the pandemic's first wave in finding a route through firms' defences.

# HOW THE PANDEMIC SHAPED COMMERCIAL ACTIVITY AND FRAUDULENT BEHAVIOUR

A very clear V-shape downturn in business

A spike in the attack rate

As well as a spike in the fraud rate



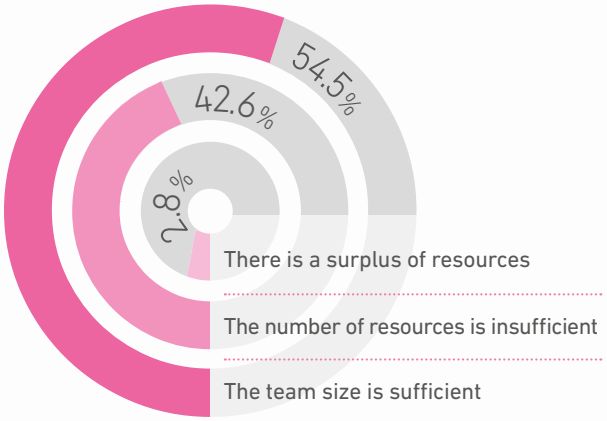
# METRICS AND KEY PERFORMANCE INDICATORS (KPIs)

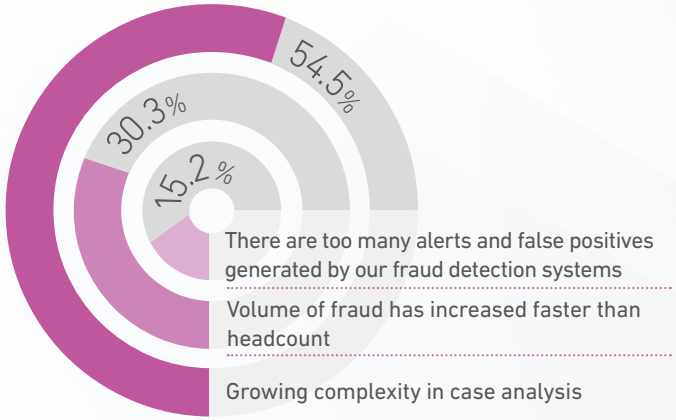
Based on experience and typical digital behaviour observed during seasonal changes, many fraud specialists knew what to expect during the pandemic. Patterns were broadly in line with the activity peaks and troughs seen during festive, pre-Christmas periods, when fraud metrics will often reflect rises in the overall volume of consumption, accompanied by a relative drop in fraud indicators.

During the lockdown, sharp declines in commercial activity were expected to drive a rise in indicators. Typically, legitimate customers will go through periods of consuming more during the run up to holidays, and less during confinement. But irrespective of that fraudsters proved they are a relentless constant and never see any reason to reduce their attempts to defraud.

Again, as highlighted, the numbers broadly reflected the forecast. As business volumes showed a V-shape, or so-called 'hockey-stick' with a low point towards the end of the lockdown period, residual fraud and related attack rates showed a symmetrical inverted V-shape with no evident fall in activity. But it's worth noting that a flat reading of data could easily lead to misinterpretations, hence the crucial importance of ensuring clear, well-designed analysis and informed reporting.

# Resolving resourcing challenges




**What do you think about the quality of resources allocated to fraud management at your organization?**


Nearly half (42.6%) of survey respondents believe their fraud prevention resources are insufficient.

In fact, the majority (54.5%) blame increasingly complex fraud types. Around one in three (30.3%) say the volume of fraud has increased faster than headcount, while nearly one in six decision-makers admit the frequency of false-positives is proving a challenge.

In terms of teams' skill sets, more than half (51.2%) say they are not able to handle emerging fraud threats. Of these, around one in 13 (7.5%) is already struggling to cover current fraud threats with existing resources. Just under half (48.9%) have full confidence in their fraud teams' abilities.

## ANALYSIS AND REPORTING

When it comes to fraud management, there are anecdotal suggestions performance measurement may often get ignored in favour of the prevention-detection-treatment mantra. But without properly analysing and measuring the challenge, the ability to make the best, or most appropriate decisions becomes far harder.

The fraud manager's dashboard must cover a variety of indicators including absolute values, volumes and amounts, as well as relative values including percentages, averages and medians. On the one hand, it needs to deliver a minimum base level of monitoring. On the other, it should also be able to offer insight and strategic analysis that will inform broader fraud policy, appetite and resourcing.

Without making a complete list, the following are all regarded as mandatory base-level insights, including number of events, number of alerts, number of frauds prevented, residual frauds, fraud attempts, false positives, along with cumulative amounts associated with the number of events.

Amount of losses prevented, and losses suffered should also be analysed. From this information it's possible to accurately calculate prevention rates, residual fraud rates, attack rates, false-positive rates, average transaction amounts and the all-important average fraud amount.

Each of these indicators, must also be delivered according to a variety of relevant analysis axes covering channels, products, geographies, points of sale, customer segment, amount segment, and so on.

They also need to be reviewed within an appropriate time frame. Some are essential to review daily, simply for operational reasons and the need for immediate tactical decisions. Others may favour monthly analysis, to help offer a cold, hard look at trends and subsequent policy readjustments. Monthly indicators should also be reviewed within a year-to-date context. Annualised ratios are important as they offer a valuable snapshot of how performance is evolving, as well as handy insight into the impact of timely and historic adjustments.

In-depth performance measurement is a highly dynamic discipline and readily orients towards decision and action. All ratios should, as far as possible, have a volume aspect, based on the number of events, and a value aspect based on the cumulative value of the same events.

As for the right level of performance for each indicator, there is no right or wrong value. It's subjective and depends on numerous alternative factors including risk appetite and tolerance, the operational capacity to handle manual reviews, automation, digitisation, reputational matters, among many others.

As an example, an alert rate requiring a manual review of 10% may be perfectly viable when there's a maximum of 200 events to process per day, as it could be easily handled by one full-time staff member. But it's inconceivable for a business generating 200,000 events per day - even if there were 100 full-time earners available.

## REGIONAL PERCEPTIONS OF RESOURCING LIMITATIONS

Across EMEA, there's a broad consensus among nearly half (**42.6%**) of all fraud teams that their resources are insufficient. But some surprising regional differences have also emerged, most notably in Spain and France, where more than two-thirds (**72.4%** and **61.5%**) of respondents voiced concern at insufficient fraud budgets. Elsewhere, Italy and Turkey were at the opposite end of the spectrum, with only around one in four (**28.6%** and **23.1%**) firms saying their fraud resources were insufficient.

Given in South Africa, a third (**33.3%**) of respondents believe their fraud teams are understaffed, senior decision-makers are urged to consider an end-to-end review of their fraud landscape. It may subsequently reveal that rules engines and processes are not consistently refined, or sufficiently flexible to deal with changes in business strategy, creating high false-positive rates. On-going lockdown restrictions are also adding a layer of complexity - often limiting investigation analysis. The lack of resources and tools also adds further complexity to fraud investigations.

In Germany, as with a number of European countries, fraud on digital channels proved particularly challenging. It spiked during the height of the pandemic, with more than half (**55%**) of respondents reporting higher fraud volumes.

In France, fraud via physical channels (**26%**) continues to outstrip fraud via digital channels (**21%**) again highlighting the importance of multi-channel and linked fraud prevention solutions.

## A QUESTION OF BALANCE

Findings showed that nearly half (49.1%) of all respondents admit they need to adopt a balanced approach. Clearly, it's a challenge if referral capacity is constrained by resources - even at a time like this when fraud attack rates are on the rise - because it's unlikely risk appetites can be changed overnight.

It's also fair to say the fraud attack rate is often the most straightforward metric to calculate. But it's one that consistently gets overlooked. It's simply the ratio of total fraud attempts to overall business volumes, set within any given timeframe.

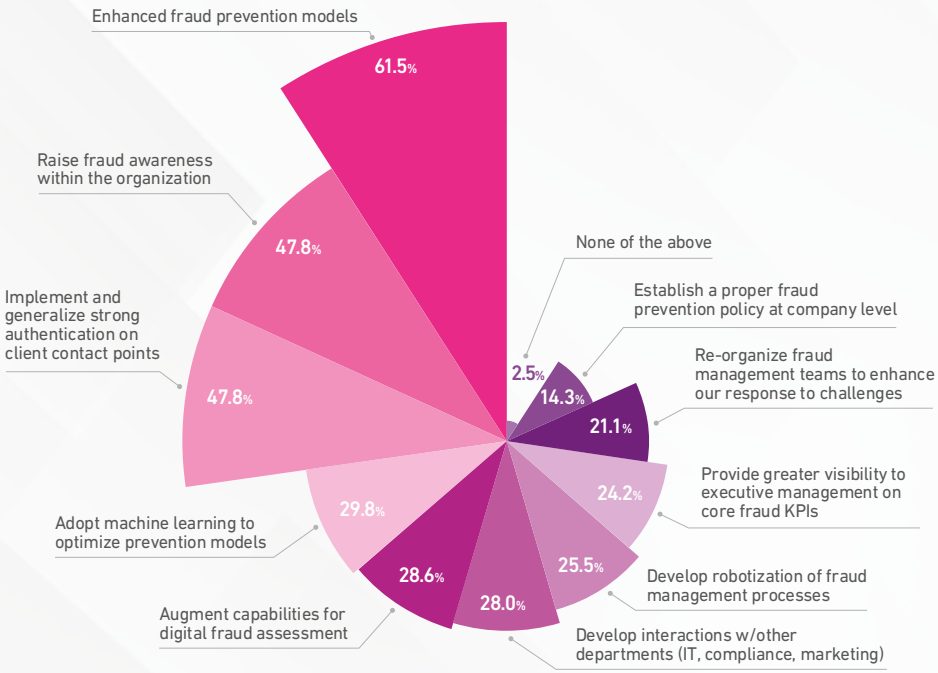
But since it combines successful and unsuccessful fraud attempts, it tends to get less attention when it comes to reporting because all the focus is diverted on to the big number of total fraud losses. Sadly, even when it is reported, this metric often sits on the side lines because businesses still believe it is dictated by the whims of criminals and criminal enterprises.

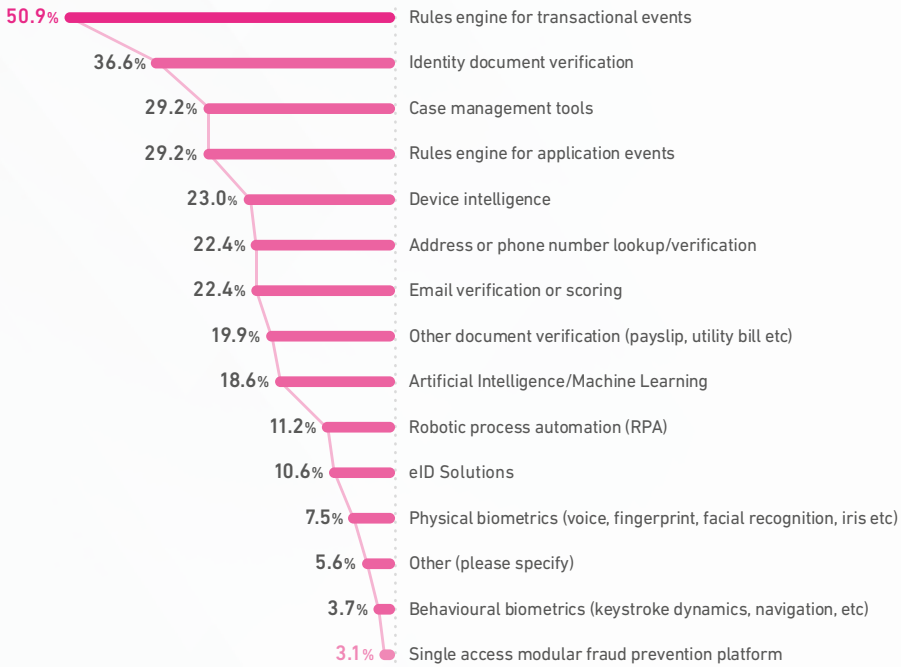
## ROUTES TO REDUCING REFERRALS WHILE INCREASING DETECTION

Multi-layered fraud mitigation solutions that combine as many available data points as possible, alongside AI and machine learning techniques are fast steps towards cutting fraud losses. They can be adopted by almost any business but should meet the following minimum benchmarks.

- Contain a robust risk engine that includes an accurate reporting module
- Include device identification technology, since so many transactional touchpoints can be easily spoofed - including, IP address, PII data and more
- Include geolocation indicators that can be collected and leveraged for risk mitigation, providing a view into the origin of the transactional event versus relying on user entered data
- Incorporate machine learning models that can maximise the fraud capture rate using all available data
- The ability to integrate other industry solutions such as biometrics, email reputation and document verification, to make the entire fraud solution so difficult to penetrate that fraudsters are ultimately obliged to go elsewhere, allowing organisations the freedom to focus on what they do best - serving their consumers

# Aspirations and key investment planning



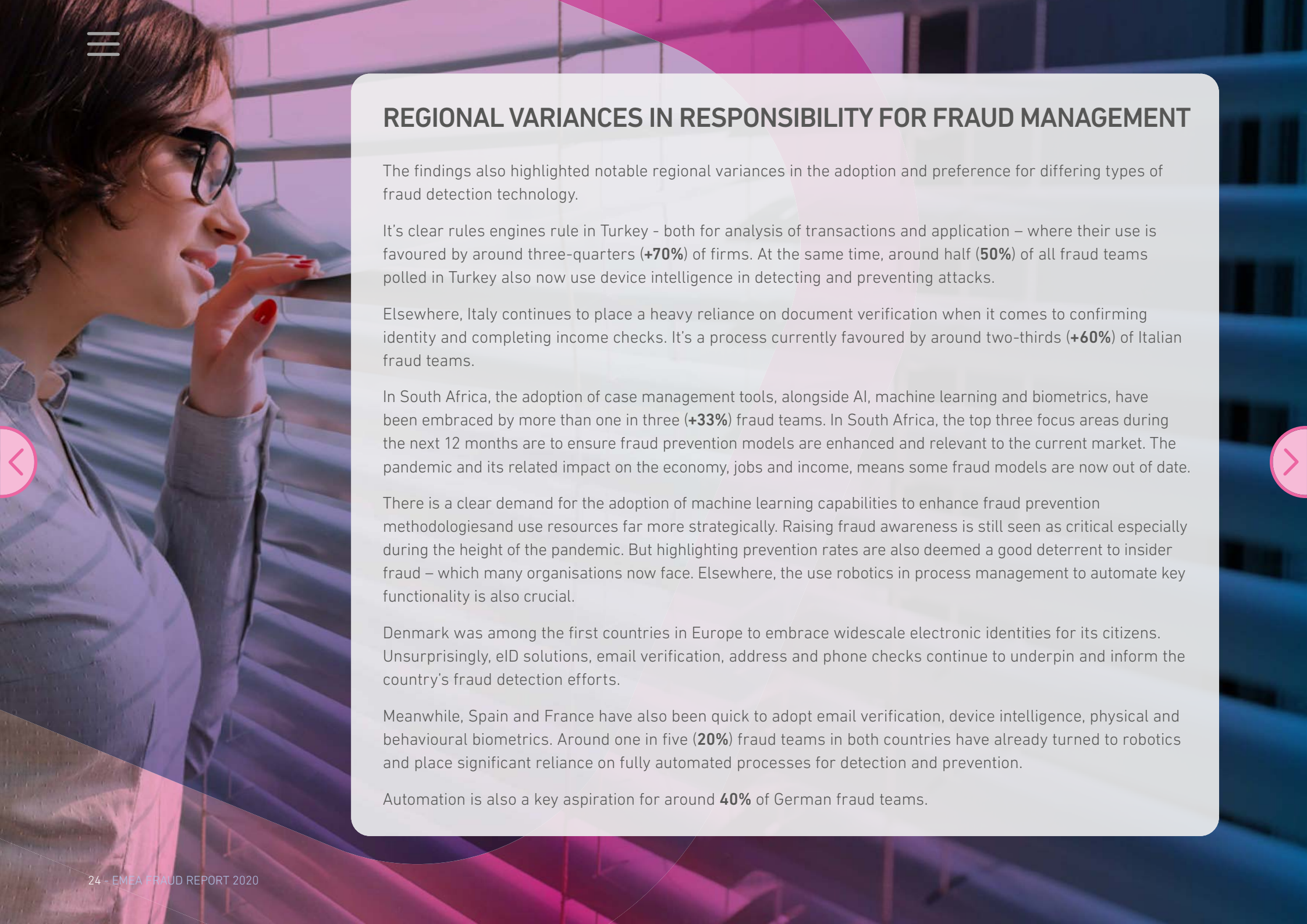

## FRAUD INITIATIVES EARMARKED FOR ADOPTION WITHIN THE NEXT 12 MONTHS

Enhanced fraud prevention (61.5%) and the adoption of machine learning to help further optimise models (47.8%) are the two key aspirations for fraud teams within the next year. But there's also a clear determination to raise know-how and the profile of fraud prevention activity within nearly half (47.8%) of all firms polled. Concern and sentiment around siloed working is also evident, with more than one in four teams (28%) keen to improve interactions with other departments, including IT, compliance and marketing.

We also asked respondents to give insight into their technological aspirations with an indication of where they would like their fraud teams to work towards. Improvements to rules engines and real-time analysis of transactions was key for more than half (50.9%).

But it's also worth noting innovations like device intelligence, email verification, AI, machine learning and greater automation, are each seen as priorities for around one in five fraud teams.

Digital fraud assessments are already being successfully augmented by the combination of device intelligence and email scoring.



# REGIONAL VARIANCES IN RESPONSIBILITY FOR FRAUD MANAGEMENT

The findings also highlighted notable regional variances in the adoption and preference for differing types of fraud detection technology.

It's clear rules engines rule in Turkey - both for analysis of transactions and application – where their use is favoured by around three-quarters (**+70%**) of firms. At the same time, around half (**50%**) of all fraud teams polled in Turkey also now use device intelligence in detecting and preventing attacks.

Elsewhere, Italy continues to place a heavy reliance on document verification when it comes to confirming identity and completing income checks. It's a process currently favoured by around two-thirds (**+60%**) of Italian fraud teams.

In South Africa, the adoption of case management tools, alongside AI, machine learning and biometrics, have been embraced by more than one in three (**+33%**) fraud teams. In South Africa, the top three focus areas during the next 12 months are to ensure fraud prevention models are enhanced and relevant to the current market. The pandemic and its related impact on the economy, jobs and income, means some fraud models are now out of date.

There is a clear demand for the adoption of machine learning capabilities to enhance fraud prevention methodologiesand use resources far more strategically. Raising fraud awareness is still seen as critical especially during the height of the pandemic. But highlighting prevention rates are also deemed a good deterrent to insider fraud – which many organisations now face. Elsewhere, the use robotics in process management to automate key functionality is also crucial.

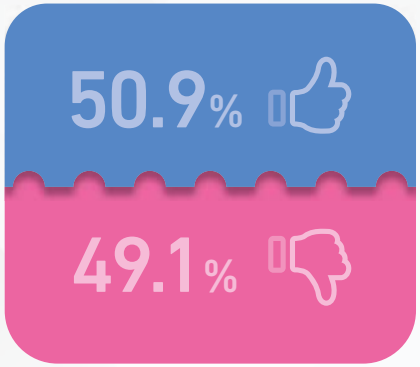
Denmark was among the first countries in Europe to embrace widescale electronic identities for its citizens. Unsurprisingly, eID solutions, email verification, address and phone checks continue to underpin and inform the country's fraud detection efforts.

Meanwhile, Spain and France have also been quick to adopt email verification, device intelligence, physical and behavioural biometrics. Around one in five (**20%**) fraud teams in both countries have already turned to robotics and place significant reliance on fully automated processes for detection and prevention.

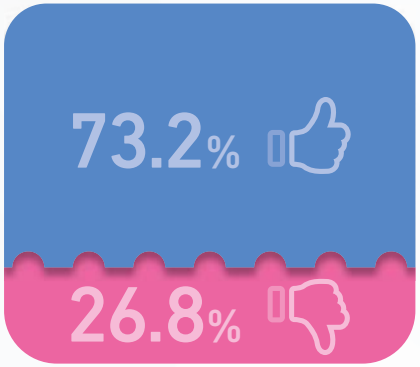
Automation is also a key aspiration for around **40%** of German fraud teams.

# The question of consortia

Do you think it would be beneficial?




Then why aren't you part of one?

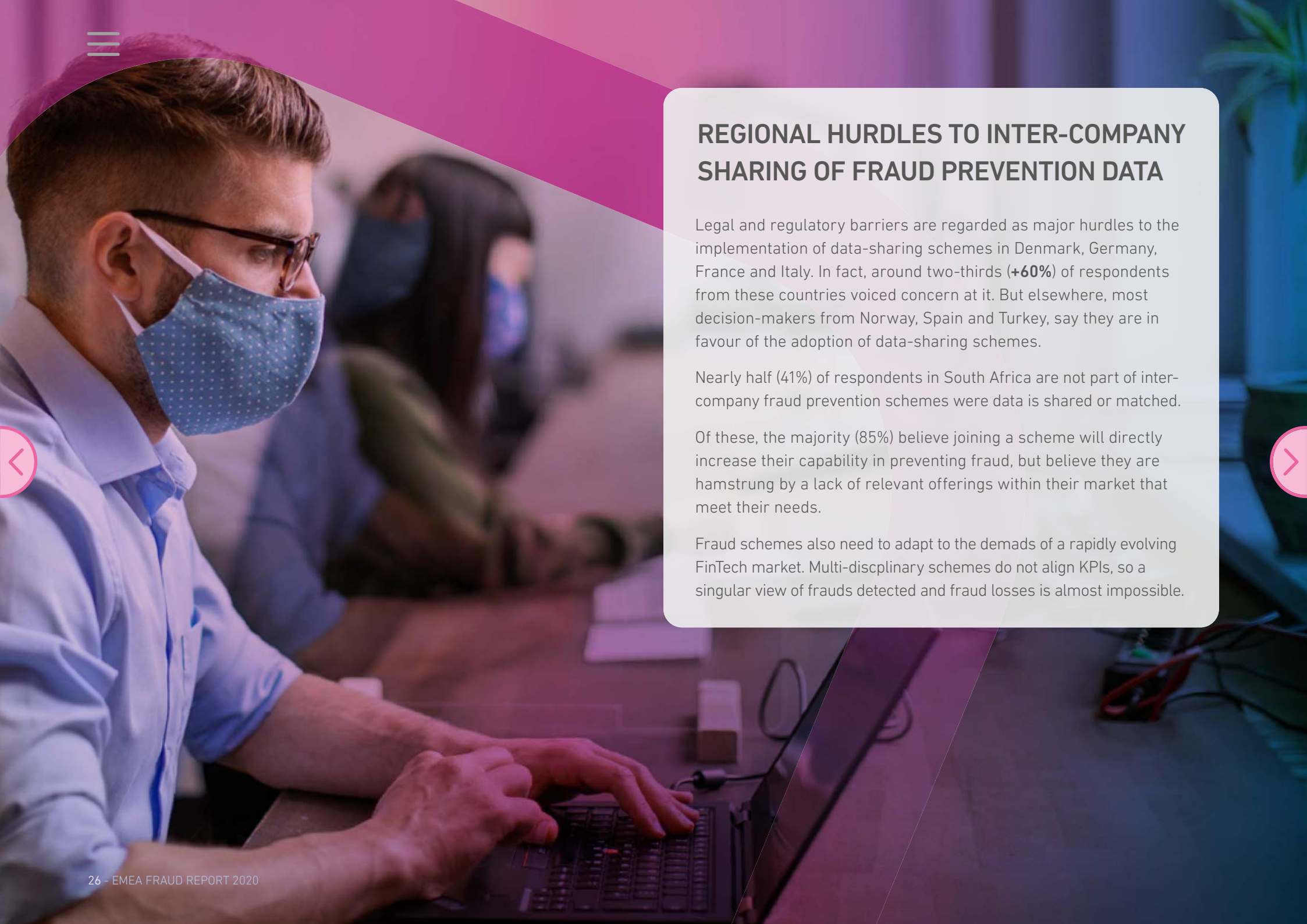



We also set out to gauge the appetite among firms for greater adoption of inter-company sharing of known fraud data in supporting detection and prevention. While just over half (50.9%) of respondents say they are currently in favour of it, success clearly hinges on unlocking regulatory obstacles to ensure delivery of a consistent solution.

Of the respondents who said they weren't yet part of a data-sharing initiative, nearly three-quarters (73.2%) favoured being part of one and readily acknowledged the benefits. Reasons given for not joining a consortium are shown in the far right-hand section, with regional regulations seen as a key blocker for around half.


## +45%

From our experience in running fraud consortia around the world for more than 20 years, we typically see that organisations will record a **45% improvement** in fraud management metrics when participating in a data consortium compared to screening exclusively against their own data.



# REGIONAL HURDLES TO INTER-COMPANY SHARING OF FRAUD PREVENTION DATA

Legal and regulatory barriers are regarded as major hurdles to the implementation of data-sharing schemes in Denmark, Germany, France and Italy. In fact, around two-thirds (**+60%**) of respondents from these countries voiced concern at it. But elsewhere, most decision-makers from Norway, Spain and Turkey, say they are in favour of the adoption of data-sharing schemes.

Nearly half (41%) of respondents in South Africa are not part of inter-company fraud prevention schemes were data is shared or matched.

Of these, the majority (85%) believe joining a scheme will directly increase their capability in preventing fraud, but believe they are hamstrung by a lack of relevant offerings within their market that meet their needs.

Fraud schemes also need to adapt to the demads of a rapidly evolving FinTech market. Multi-discplinary schemes do not align KPIs, so a singular view of frauds detected and fraud losses is almost impossible.

# Capabilities and conclusion

Fraud is a global challenge and it's one we're helping our strategic clients with daily.

We're delivering it through consultancy services, including prevention strategies, anti-fraud policies, process reviews and more directly through solutions designed to detect and prevent multiple fraud types.

It's also worth noting our technology is transparent, with fraudsters often unable to spot or anticipate it, leaving the likelihood of circumvention very low. It also delivers real-time device and connection analysis, behaviour analysis and behavioural biometrics at the point of log-in. Added to that are insight into typical account behaviour and ongoing analysis of events on key data points, such as IBAN, phone number, email address, and more - all via very advanced rulesets.

From a customer experience stand-point the technology is near-seamless - and in many instances can speeds up the homepage to checkout journey. Adopting a holistic approach to analysis of a given series of elements, rather than just one, offers far more robust protection to customers and our clients.

As we've seen with the re-emergence of Sim-swap, phishing and the on-going threat of account takeover, fraudsters are determined, opportunistic and continually testing fraud defences with differing techniques. But clearly, when there are numerous vulnerabilities and multiple risk-factors, systematic and strategic approaches are required. On the one hand to ensure maximum detection and prevention, balance security and customer experience, while on the other hand maintaining agility and responsiveness to new or emerging threats.

### Increase customer trust and recognition

By optimising data acquisition and enrichment.

### Improve detection and prevention

By adopting machine learning-driven predictive analytics that can deliver real-time client support with customer risk treatments at every interaction.

### Fight new and emerging fraud types

Through smart orchestration, integration and automation of multi-layered identity and fraud solutions.

**Austria**
Strozzigasse 10/14
1080 Vienna
www.experian.at

**Bulgaria**
Space Tower
86 Tsarigradsko Shosse Blvd
Sofia 1113
www.experian.bg

**Denmark**
Lyngbyvej 2
2100 Copenhagen
www.experian.dk

**France**
Tour PB5
1 avenue du Général de Gaulle
La Défense 8
92074 Paris La Défense Cedex
www.experian.fr

**Germany**
Rheinstraße 99
76532 Baden-Baden
www.experian.de

**Greece and Romania**
65 Ag. Alexandrou Street
17561 Paleo Faliro Athens
www.experian.gr

**Italy**
Piazza dell'Indipendenza, 11/b
00185 Roma
www.experian.it

**Netherlands**
Grote Marktstraat 49
2511 BH, Den Haag
Postbus 13128, 2501 EC, Den Haag
www.experian.nl

**Norway**
Karenlyst Allè 8B, 0278 Oslo
Postboks 5275, Majorstuen
0303 Oslo
www.experian.no

**Poland**
Metropolitan Complex
Plac Pilsudskiego 3
00-078 Warsaw
www.experian.com.pl

**Russia**
5, bldg. 19, Nizhny Susalny lane
105064 Moscow
www.experian.ru.com

**South Africa**
Ballyoaks Office park
35 Ballyclare Drive
2191 Bryanston, Sandton
www.experian.co.za

**Spain**
Calle Príncipe de Vergara, 132
28002 Madrid
www.experian.es

**Turkey**
River Plaza
Buyukdere Cad. Bahar Sok.
No: 13 Kat: 8 Levent
34394 Istanbul
www.experian.com.tr

**United Arab Emirates**
Dubai Islamic Bank Building 01
Office 102, First Floor
Dubai Internet City
www.experian.ae

**Registered office address:**
**The Sir John Peace Building, Experian Way,**
**NG2 Business Park, Nottingham, NG80 1ZZ**

**T: 0844 481 5873**
**www.experian.co.uk**



21-EMEA-0022