Ravelin

ONLINE MERCHANT PERSPECTIVES

FRAUD & PAYMENTS SURVEY 2022

ravelin.com

CONTENTS

1.0 INTRODUCTION

Overall, 2021 was another turbulent year for ecommerce. New Covid variants emerged, causing staggered recovery across the world. Despite the tentative return of in-person buying, ecommerce continued to boom, and it became clear that the digital shift isn't going anywhere.

But with rising digital sales came increasing fraud attacks. New types of fraud are still emerging, as fraudsters continue to hone their methods, take advantage of weaknesses caused by the Covid outbreak, and explore tactics that side-step 3DS.

In this report, we compare data from 2020 to results taken in 2021. How has your experience of fraud changed over the year? What impact have regulations like Europe's PSD2 had on fraud and conversion rates?

This report provides insights into:

- Merchant perceptions of how fraud is changing and top business threats
- Tools, budgets and methods for monitoring fraud
- Wider environmental factors, including Covid-19 and PSD2

Survey methodology

These quantitative surveys were commissioned by Ravelin and carried out by Qualtrics.

The 2020 data came from 1,000 fraud professionals from countries around the world. The 2021 survey was carried out using a panel of 1,700 global fraud professionals. Survey participants work for online merchant businesses with more than $50 million in annual revenue. The survey was translated into each respondent's local market language for clarity.

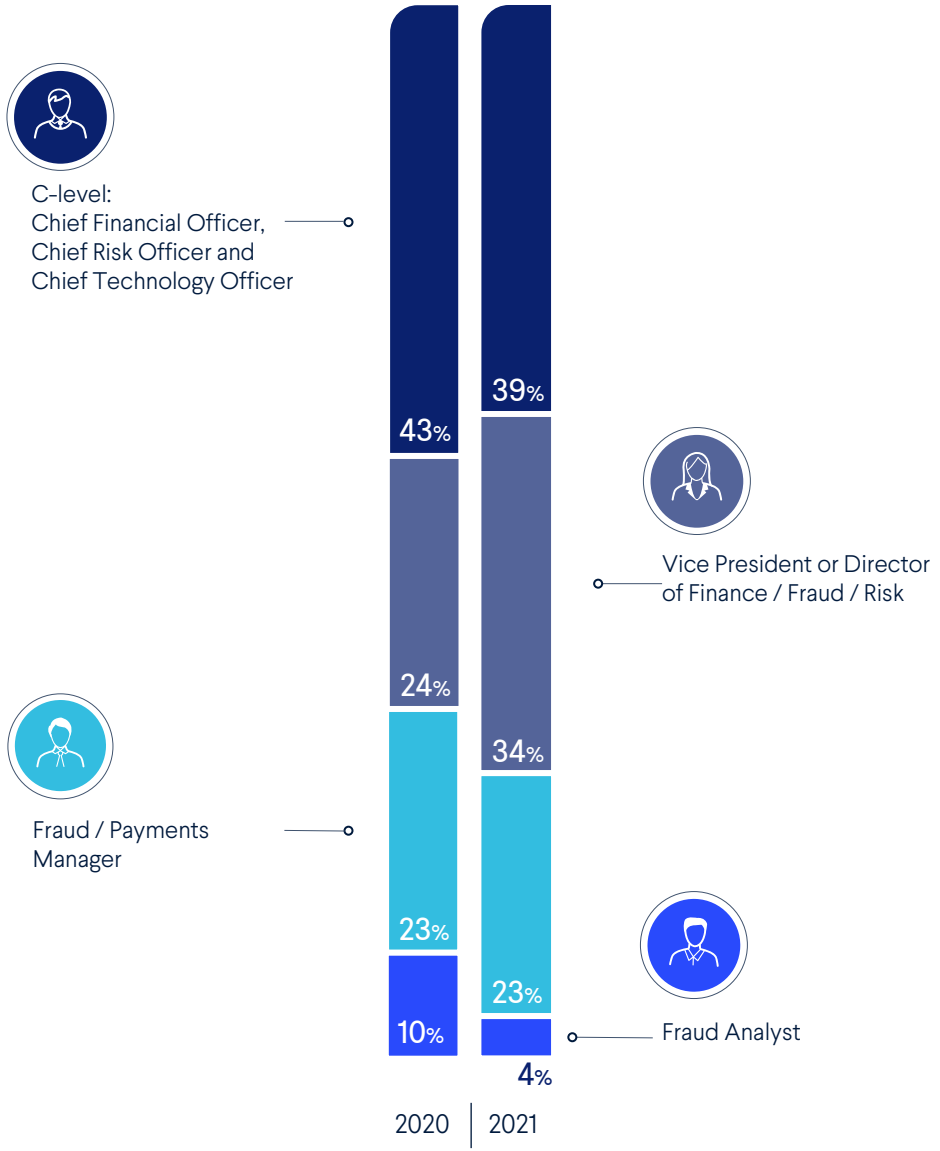
2.0 SURVEY SAMPLE

Industry, location and job roles

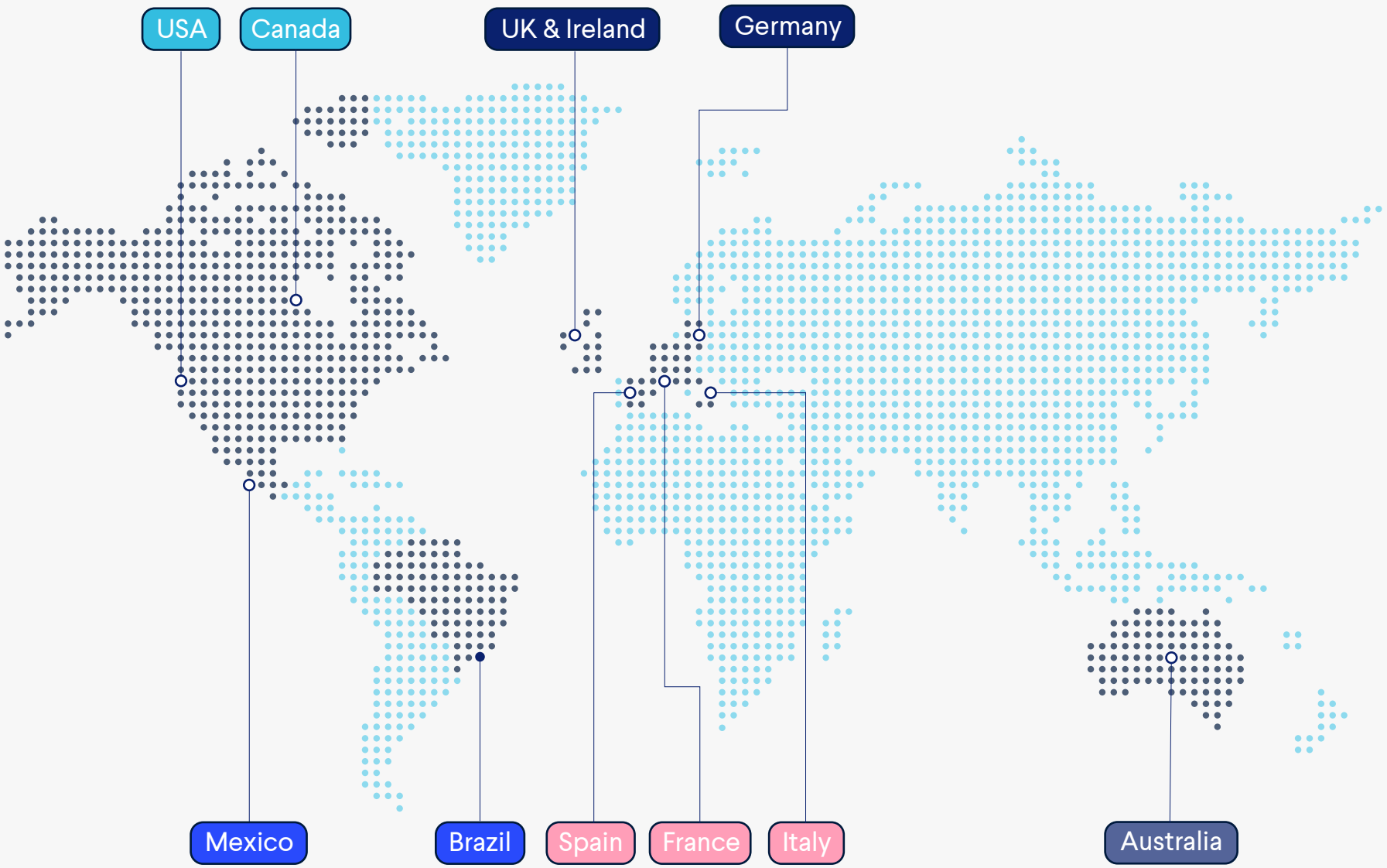
Survey participants are fraud and payments professionals from around the globe. These professionals work in key ecommerce markets in Australia, Europe, and North and South America. Survey participants work in a range of business industries under five main groups: Retail, Travel & Hospitality, Digital Goods, Marketplaces and Subscriptions.

All participants work in a fraud-related role, from Fraud Analyst up to Chief Financial Officer. Two-thirds of participants come from senior roles, with around 40% at C-level.

SURVEY PARTICIPANT **JOB TITLES**



SURVEY PARTICIPANT **COUNTRIES**



SURVEY PARTICIPANT **INDUSTRIES**

3.0 THE COVID-19 EFFECT

ALMOST **20%** merchants said Covid impact has been positive

Travel restrictions, curfews and precautions are still in place **around the world**, causing continued disruption to ecommerce. We asked how has the impact of Covid-19 changed over the past year for your business?

The majority said it's been positive! In 2021, almost 20% more merchants said the pandemic has been positive compared to the previous year.

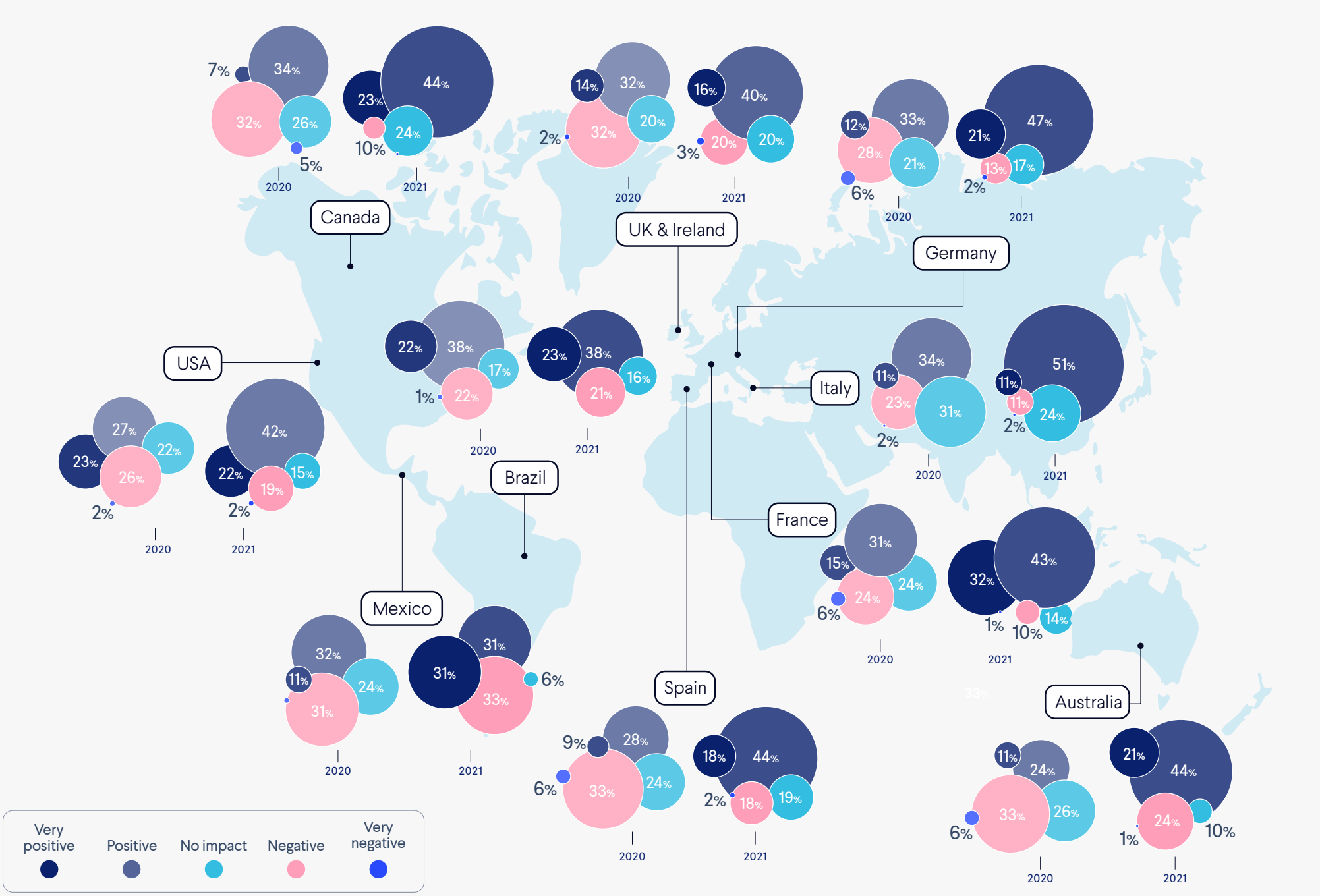
Impact of Covid-19 by country

Around 75% of merchants in France have now said the effect has been positive, up from 46% in 2020. The pandemic majorly boosted the ecommerce market in France, and it's now **the seventh largest in the world.** While in 2020 many businesses were overwhelmed by the accelerated digital shift, in 2021 merchants have likely adjusted to the new climate.

Brazil is an outlier, as merchants based there haven't seen positivity increase over the year. Brazil has been named '**the epicenter of the global outbreak**', and in 2021 they were still in the thick of pandemic disruptions. This may have put Brazil-based merchants a step behind those based in countries like France that are now settling into business as usual.

Mexican merchants are most likely to say the pandemic has had a negative impact. This is no surprise, as we'll later discuss, fraud rates in Mexico are rising faster than any other country in the survey.

IMPACT OF COVID-19 BY **COUNTRY**



Impact of Covid-19 by industry

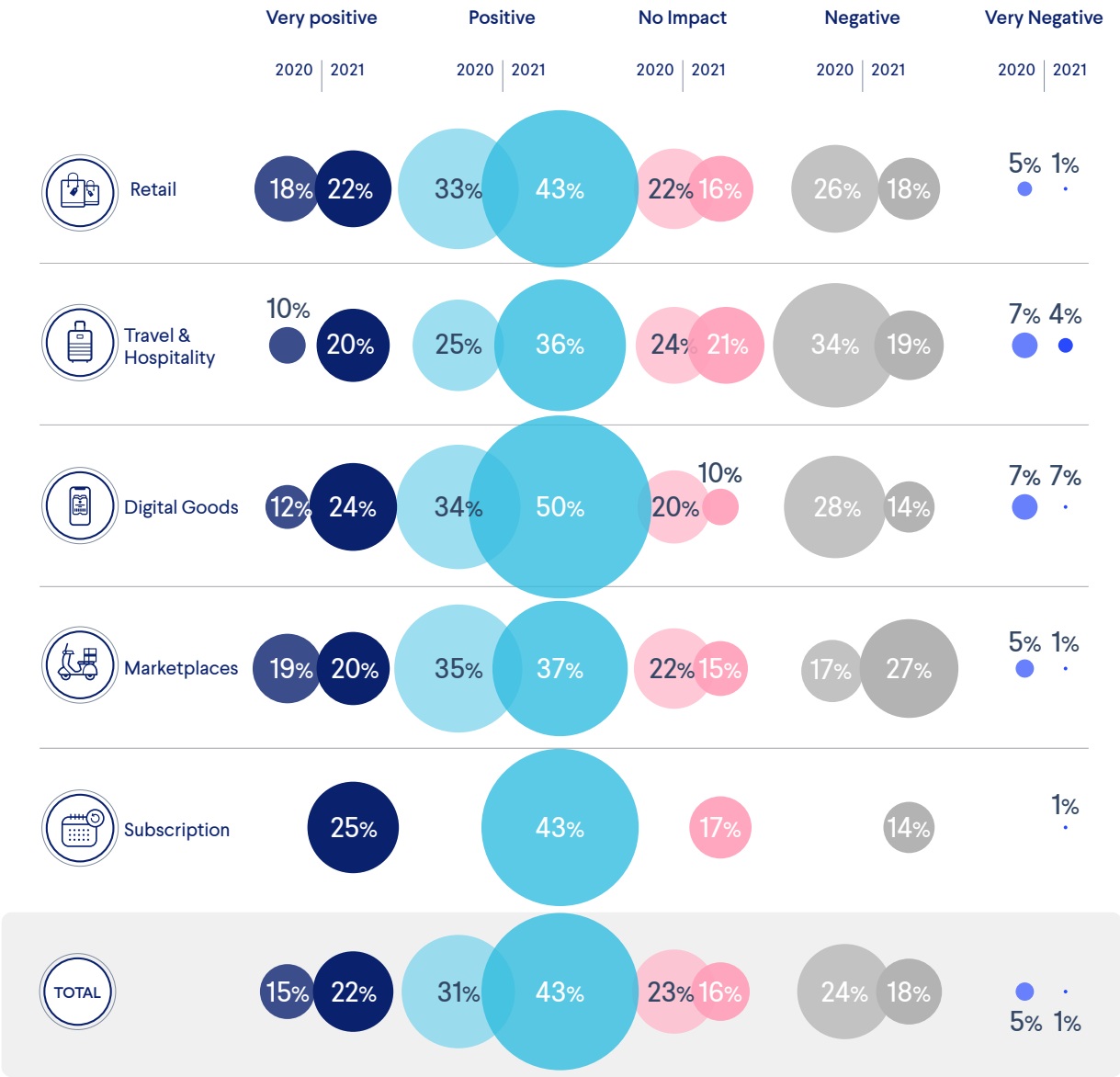
How has the Covid-19 outbreak impacted your industry compared to the rest of ecommerce? It's a mixed bag, as every business type faces unique challenges.

More Digital Goods and Subscription merchants saw a positive impact than other industries. Over half have also said they've seen order volumes skyrocket. Marketplaces, particularly food delivery merchants, are most likely to say the impact has been negative, which, as we'll later discuss, could be due to declining profits.

Travel & Hospitality merchants have had the biggest change of heart since 2020. The proportion who said the Covid impact was very positive doubled, and those who said it was negative almost halved. But the industry's overall view is still less positive than others.

The industry may be cautiously positive because business started to recover in 2021 but not fully. Air reservations **were still down 86%**, and many travel professionals don't expect full recovery until **at least 2024**.

IMPACT OF COVID-19 BY **INDUSTRY**



3.1 HOW HAS THE PANDEMIC IMPACTED EACH INDUSTRY?

We asked merchants to get specific about how the pandemic has affected business. Have your profits increased? Is competition increasingly tough? Here's what they said...

64%

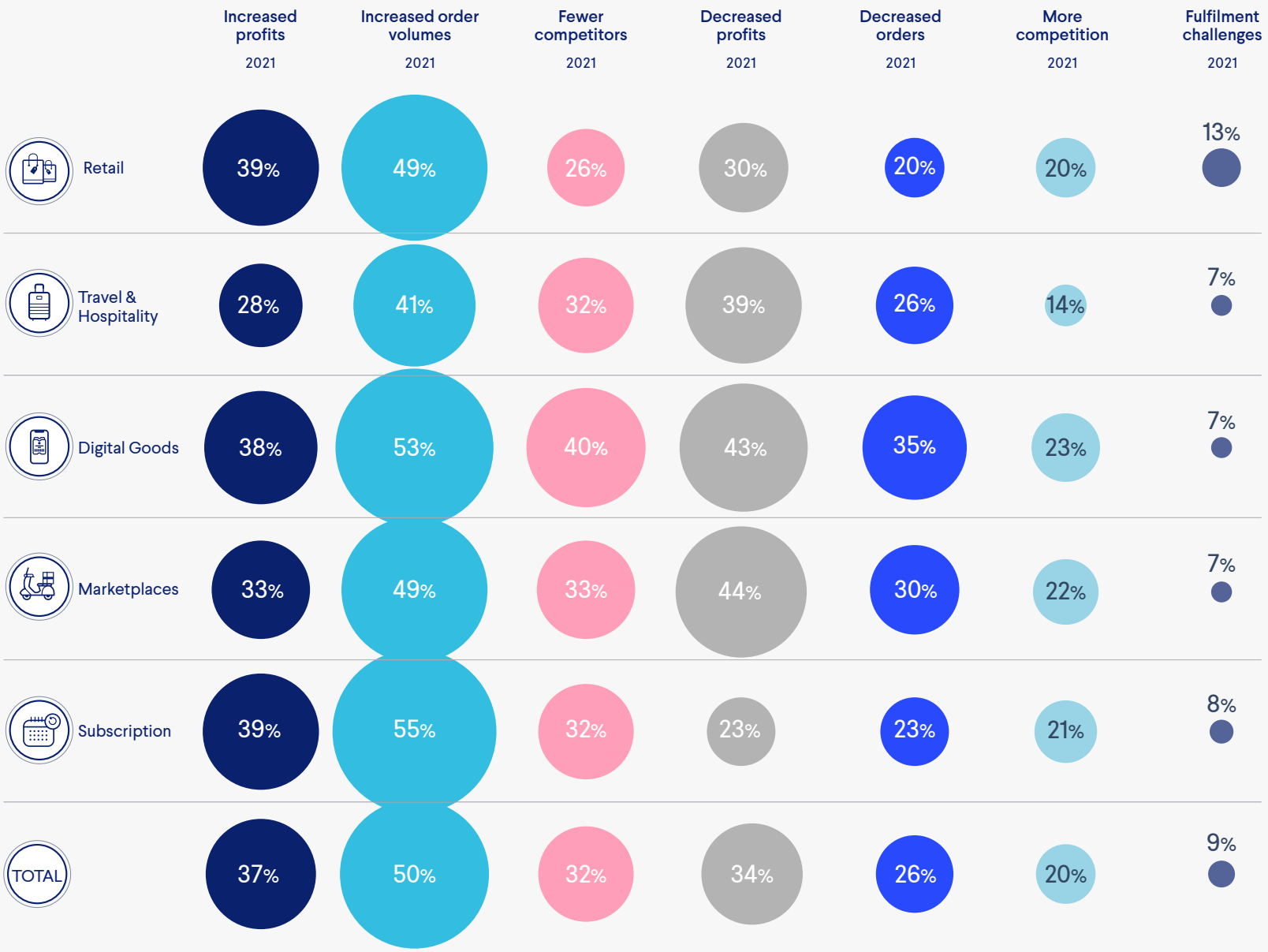
of grocery merchants are still worried about inventory

Merchants across all industries have seen order volumes increase. Physical goods subscription merchants have seen order volumes rise more than any other business types, as the pandemic massively **boosted the subscription economy**.

On average, merchants don't report that the pandemic has notably impacted fulfilment. But retailers are twice as likely to see this as an issue than other industries. Increased demand, staff shortages and port closures caused retail supply chains to bottleneck. And around **64% of grocery merchants are still worried about inventory**.

Marketplaces are the most likely to say profits have decreased, as the business model is **cost intensive and low margin**. Around 48% of taxi marketplaces have seen profits drop. In 2021, taxi use bounced back post-lockdown, but there weren't enough drivers to meet demand, as **many switched to food delivery**. Intense competition for drivers and customers alike make it difficult for taxi marketplaces to turn a profit.

HOW HAS THE PANDEMIC IMPACTED EACH **INDUSTRY?**



3.2 HOW HAVE FRAUD LEVELS CHANGED?

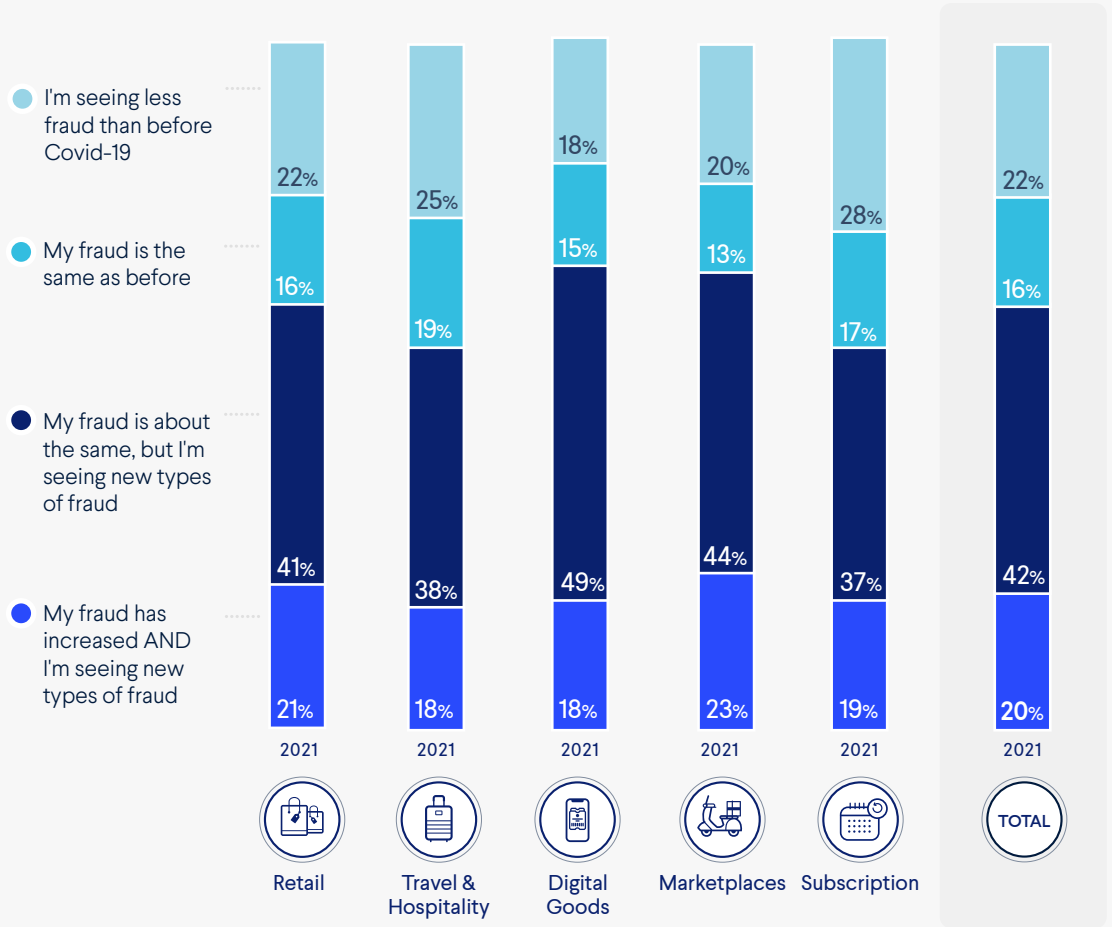
62% of merchants are seeing new fraud types emerge

How has Covid directly impacted your fraud? Most merchants said that fraud levels have stayed around the same, but new types of fraud are appearing fast.

A huge 62% of merchants are seeing new fraud types emerge. This means businesses are having to quickly add to their fraud toolbox. Under a quarter of merchants are seeing less fraud than pre-pandemic.

The responses vary for specific business types. For example, a third of Digital Goods Event Ticketing merchants are seeing fraud increase and new types of fraud. Over a quarter of Taxi/Cab marketplaces and Grocery retailers have said the same.

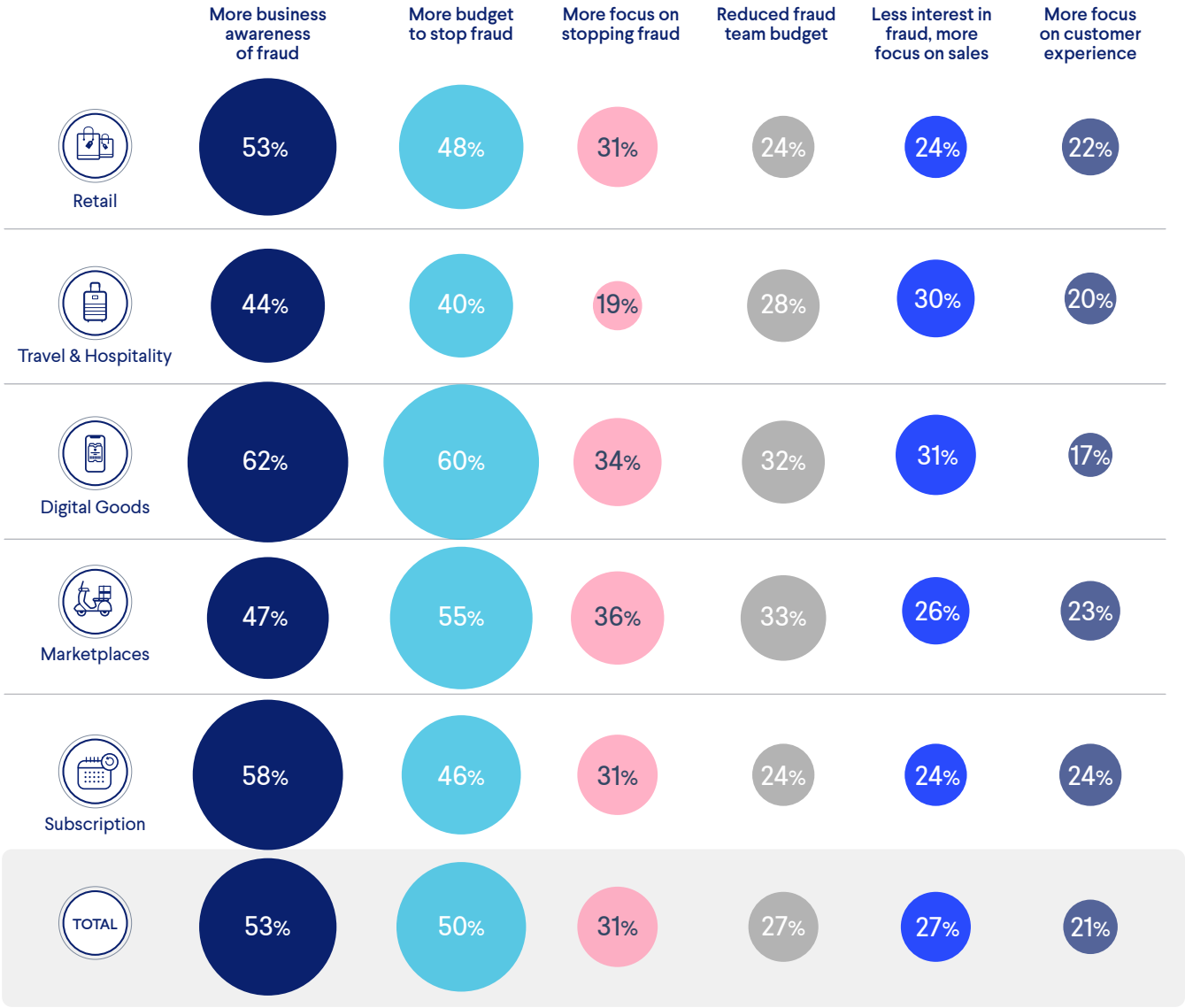
IMPACT OF COVID-19 BY **INDUSTRY**



3.3 HOW HAS YOUR BUSINESS APPROACH TO FRAUD CHANGED?

Have you seen business awareness of fraud grow throughout the pandemic? If so, you agree with 53% of the merchants we surveyed. Half of merchants have also seen an increase in their budget to stop fraud, in line with 2020 predictions.

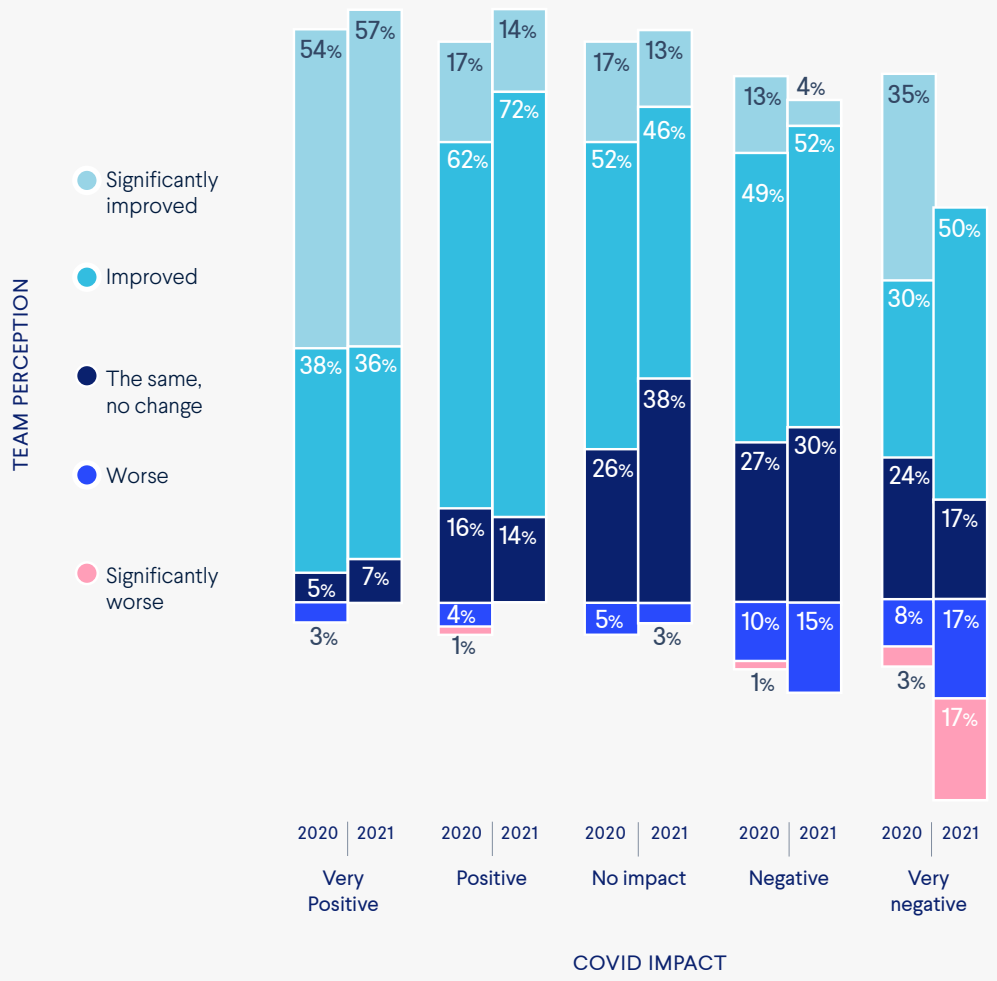
HOW HAS YOUR **BUSINESS APPROACH** TO FRAUD CHANGED?



Overall businesses seem to be focussed on stopping fraud, which is great for fraud teams! We also know that many are getting well-deserved recognition and investment, particularly from business leaders.

Of the merchants who said Covid-19 had a very positive impact on fraud team operations, 54% also said the perception of the fraud team had significantly improved in the past 12 months. Growing appreciation is likely a key factor behind the overall positivity. We also know many teams are getting well-deserved recognition from business leaders, as we'll discuss later.

COVID IMPACT ON **PERCEPTION OF FRAUD TEAM**



4.0
DID FRAUD TEAMS GROW IN 2021?

In 2020, we asked merchants to predict whether their fraud team would grow or shrink in size over the next year. Over 70% of merchants thought their fraud team would increase in 2021, and they were right.

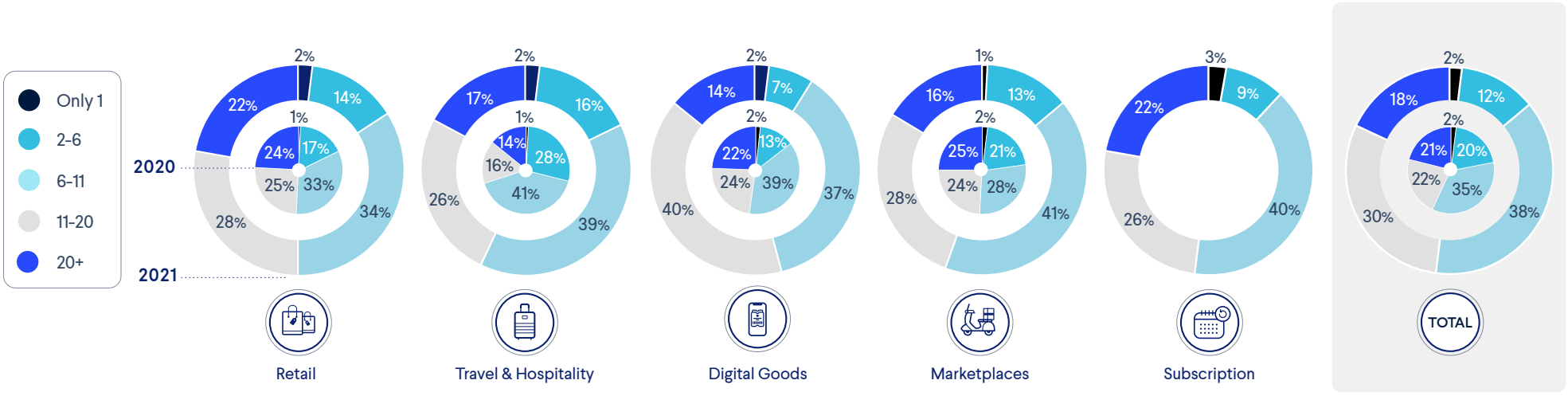
Fraud teams across all industries have grown over the past year. In 2021, 86% of merchants have a fraud team of six or more, compared to only 78% last year. And only 12% of businesses have teams from two to five people, down from 20% YoY.

Travel & Hospitality and Digital Goods fraud teams have grown the most out of all industries. Last year only 30% of Travel fraud teams had 11 or more people, but in 2021, 43% have teams this size. This is unexpected, as almost 10% forecasted a decrease.

This growth is amidst an unstable year for Travel & Hospitality. Due to global restrictions, overall passenger traffic in 2020 saw **the largest YoY decline in aviation history**, and US hotel **revenue per room** went down 20%. Against all odds, Travel & Hospitality fraud teams are still recruiting.

Digital Goods fraud teams are the largest on average, as over half have 11 or more people, up from 46% last year. Gaming and gambling industries may have had to increase their fraud protection as online transactions boomed since the Covid outbreak, making them more lucrative fraud targets than ever before.

NUMBER OF PEOPLE IN THE **FRAUD TEAM**

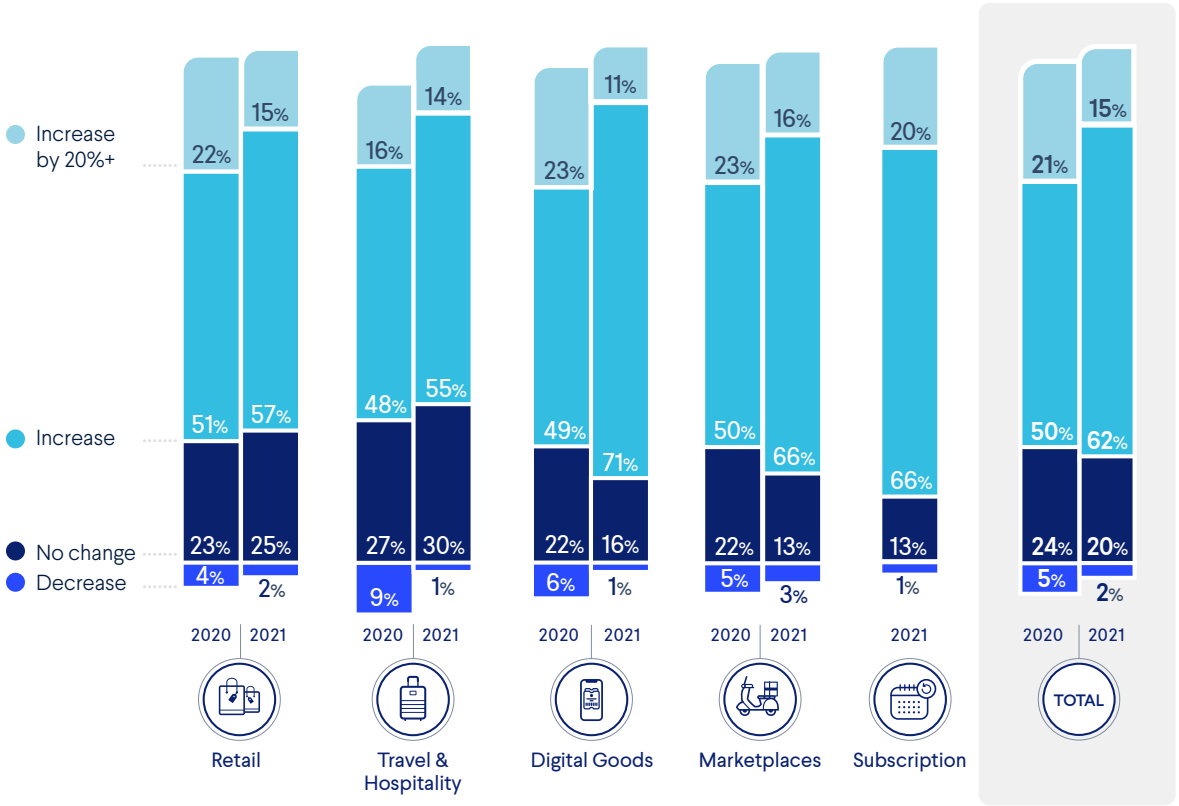


4.1 ARE FRAUD TEAMS PREDICTING FURTHER GROWTH IN 2022?

More online merchants predict their fraud team will grow over the next year than they did in 2020. Almost 80% of merchants across all industries expect further increase in 2022, compared to around 70% last year.

But merchants are expecting growth to be slightly less drastic, as fewer predict the fraud team will increase by over 20% YoY. This might be because they've already grown in the past year or that the digital acceleration sparked in 2020 is slightly slowing down. Since two-thirds of businesses think evolving online operations in the next five years is essential to survival, merchants are perhaps incorporating fraud team growth into a considered long-term strategy.

PREDICTIONS OF FRAUD TEAM GROWTH
BY INDUSTRY



4.2 PREDICTIONS OF FRAUD TEAM GROWTH BY JOB ROLE

In 2020, CFOs were most likely to predict an increase in the fraud team of all job roles. This year, CFOs have been overtaken by a huge 88% of CROs expecting growth.

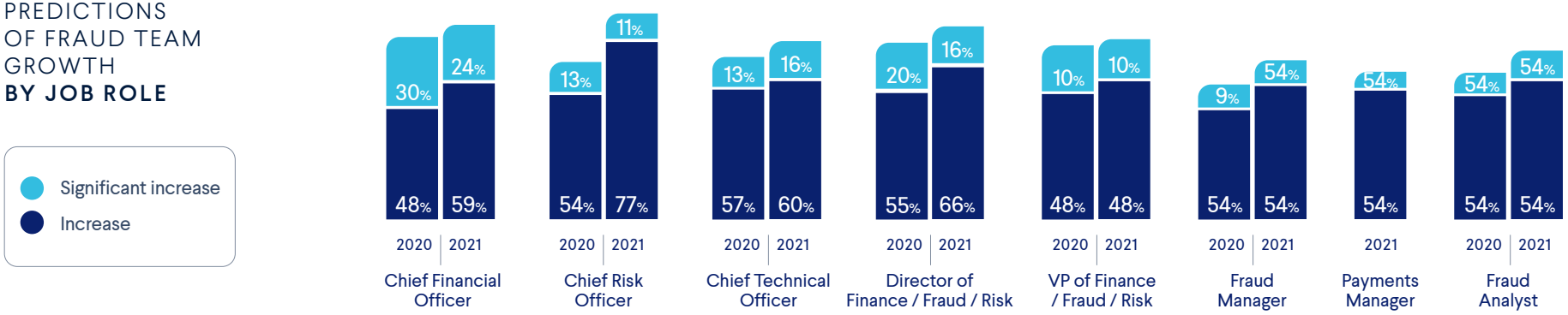
CFOs are confident about fraud team expansion in 2022, with more predicting an increase than last year. They are also still most likely to predict a significant increase, at just around a quarter of CFOs.

CFOs have shifted their focus to hiring digitally-specialized employees and **crisis-management** since the start of the pandemic. If 2021 taught us anything, it's that online growth and resilience are key to business success. Hiring and upskilling your fraud team is central to advancing online safely.

Although business leaders are most likely to predict fraud team growth, 72% of analysts are expecting an increase in the next year, which is more than the 63% in 2020. But, as we later discuss, analysts are less confident about fraud budgets increasing in 2022.

Why are analysts more optimistic about hiring than budgets in 2022? Perhaps they think more hands on deck should be prioritized over money spent on tools. Merchants may be realizing that there's always a limit to what you can automate, and as fraud becomes more sophisticated, human responses are invaluable.

PREDICTIONS OF FRAUD TEAM GROWTH **BY JOB ROLE**



4.3 FRAUD TEAM DEPARTMENT WITHIN THE BUSINESS

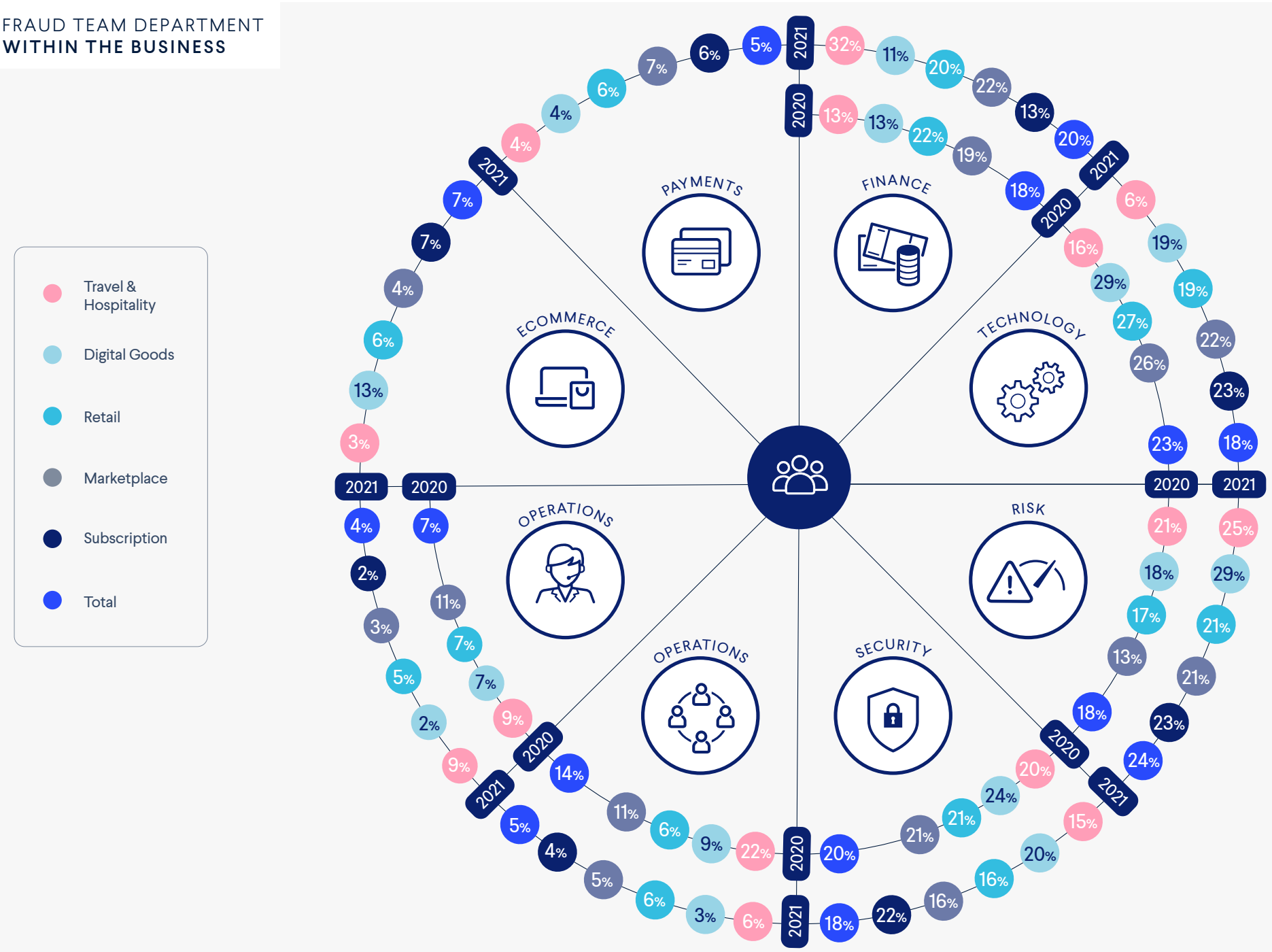
Last year, the most common home for the fraud team was the Technology department. This year, the fraud team is most likely to sit under Risk/Assurance, home for around a quarter of all fraud teams. There's a slight reduction in the percentage of fraud teams in the Tech department at 18%, down from 23% in 2020.

The name of the fraud team and its department influences the wider business perception. Changing the fraud team name or position under Risk/Assurance may help boost its ranking and make it seem more integral. This rebranding could help fraud teams shake off previous misconceptions and integrate more effectively with the wider business.

Overall, it's clear there's still no one-size-fits-all in terms of where the fraud team should sit. The broad nature of fraud means it makes sense in many areas of the business.

> "There's still no one-size-fits-all in terms of where the fraud team should sit.

FRAUD TEAM DEPARTMENT **WITHIN THE BUSINESS**



4.4 WHAT ARE YOUR FRAUD TEAM'S RESPONSIBILITIES?

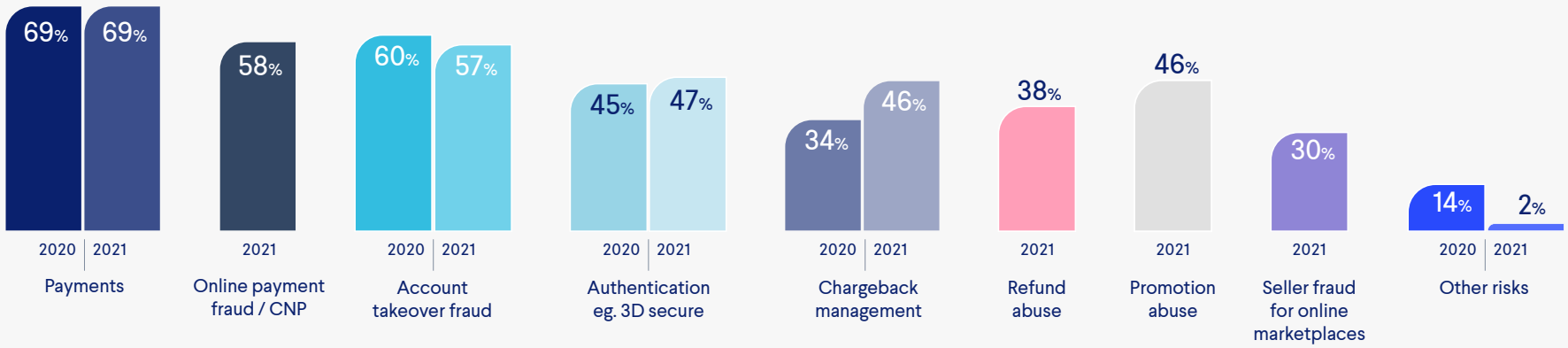
Fraud teams have a range of different responsibilities, depending on business priorities. But it's clear across industries that many key threats are managed by other teams. This means that communication with other departments is key, or you might not see the full picture of your fraud.

Only 57% of fraud teams are responsible for account takeover. This fraud type often involves multiple teams, so it can be **hard to decide who should take charge.** Poor collaboration between teams can create obstacles or delays that give hackers the upper hand. This is especially true amid the pandemic - remote workers spend **25% less time** communicating outside their team.

Refund and promotion abuse skyrocketed in 2020, but only 40% of fraud teams manage these threats. While these unprofitable behaviors aren't strictly 'fraud,' they can seriously impact your bottom-line.

Only 30% of online marketplace fraud teams are managing seller fraud. This could be due to the invisibility of the problem, as there are no easy metrics to measure the costs, so it's hard to make a case that it's a fraud team priority. Or marketplaces may be turning a blind eye to bad behavior to keep all-important sellers. Or even worse still, merchants may not be aware that seller fraud is happening.

RESPONSIBILITIES OF THE FRAUD TEAM



4.5 PERCEPTION OF THE FRAUD TEAM BY JOB ROLE

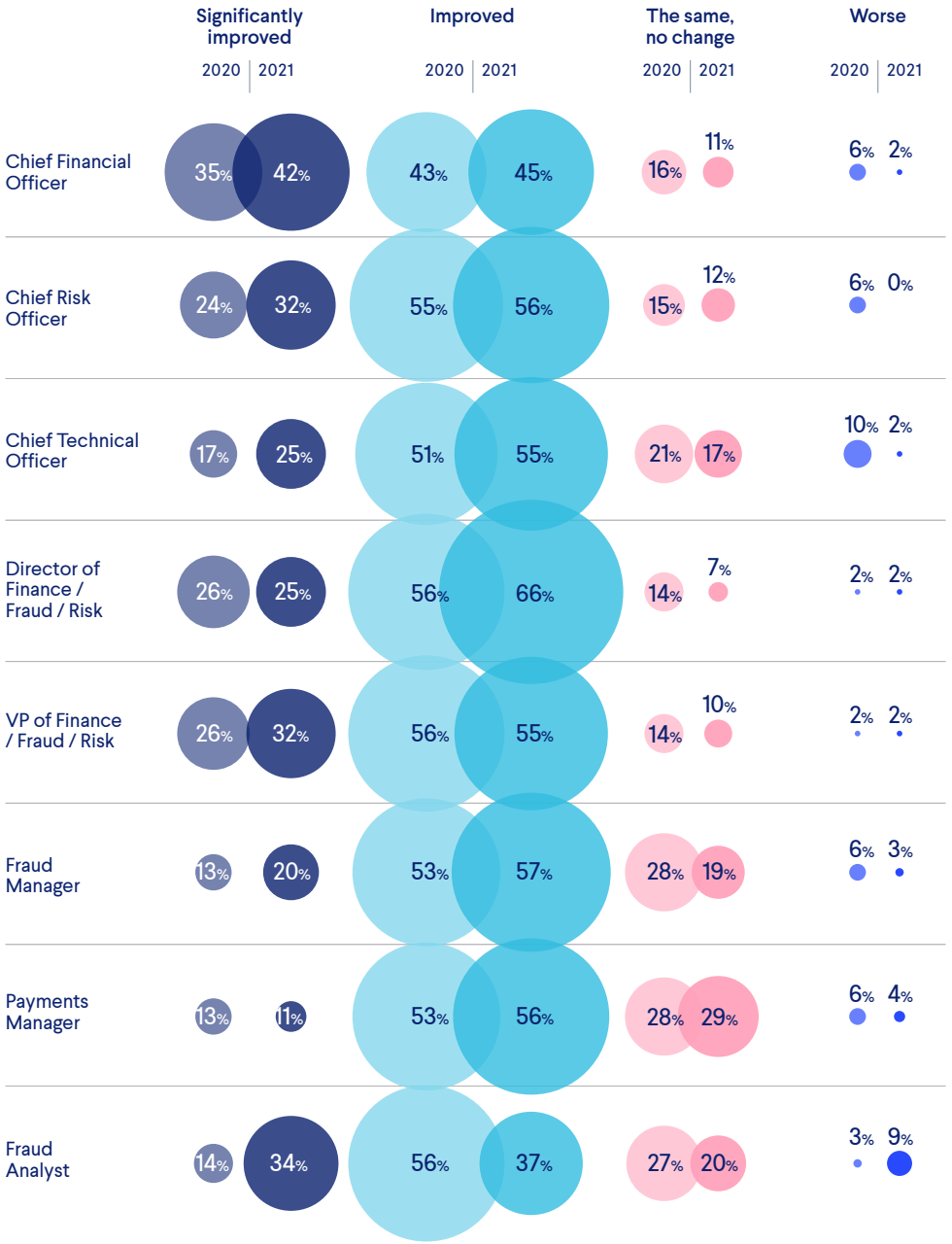
Most merchants have seen the wider business perception of the fraud team improve in the past year. This correlates with predictions of fraud team growth, and the trend that online operations are increasingly integral to business function.

Senior roles are most likely to think perception has improved. Last year, 75% of C-levels reported an improvement. In 2021, this has risen to 85%, with almost 90% of CFOs and CROs seeing a change. This is cause for celebration! Congratulations to all fraud teams for winning hard-won appreciation.

A huge 42% of CFOs report a significant improvement, compared to 35% last year. Your reputation just gets better and better, and it's a huge testament to the enduring hard work of fraud professionals amid the pandemic.

While managers and analysts are still least likely to recognise changing perception, over a third have seen significant improvement, compared to only 14% last year. Perhaps fraud teams are becoming aware of how valued they are.

PERCEPTION OF THE FRAUD TEAM
BY JOB ROLE

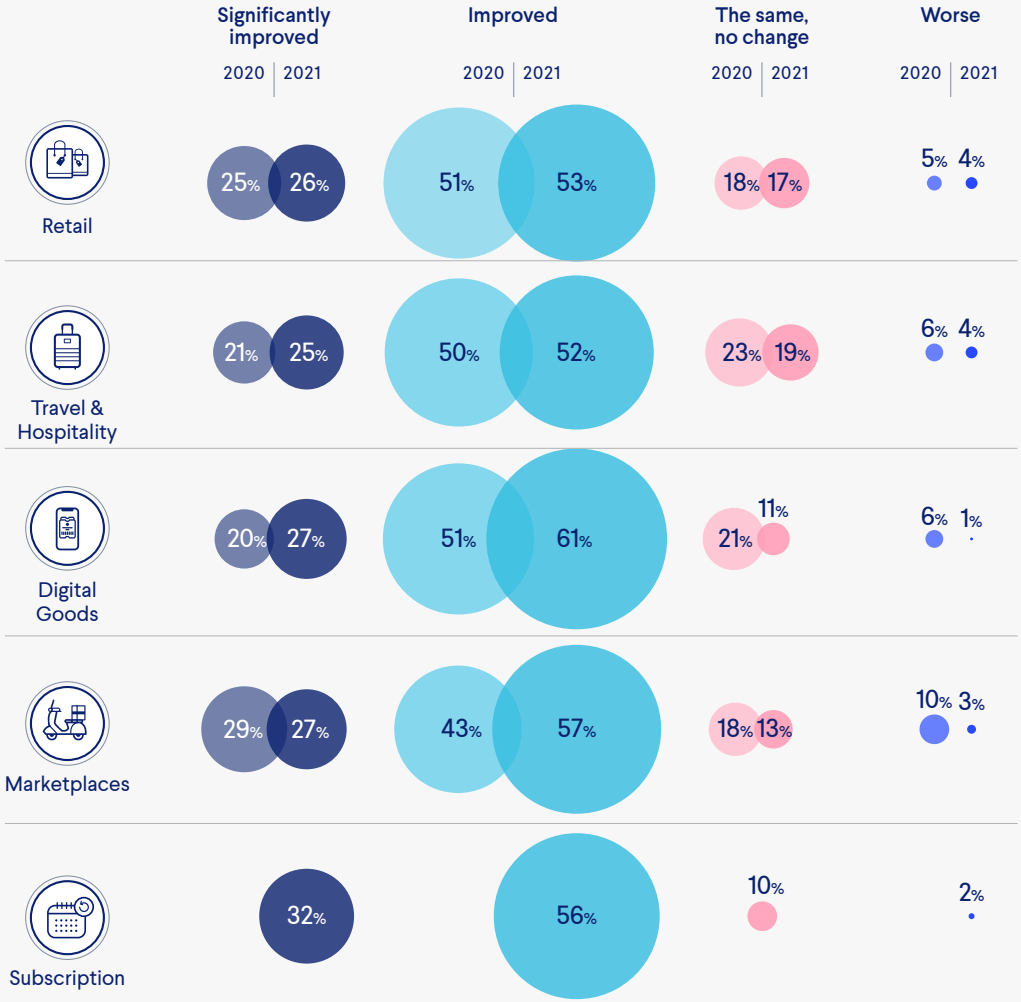


4.6 PERCEPTION OF THE FRAUD TEAM BY INDUSTRY

Overall fraud team perception has improved across all industries. Last year 10% of marketplaces said perception had worsened but in 2021 this has dropped to 3%.

Almost 90% of Digital Goods and Subscription merchants are noticing a positive change. Subscription merchants saw the most dramatic improvement, as a third said perception improved significantly. This could be because subscriptions have become mainstream since the Covid outbreak - lifelines for isolating customers looking for excitement. **Subscribers to digital news and media grew 300%** and **one in five US customers bought a subscription box in 2020**. If your digital popularity grows, your fraud team becomes more important.

PERCEPTION OF THE FRAUD TEAM **BY INDUSTRY**



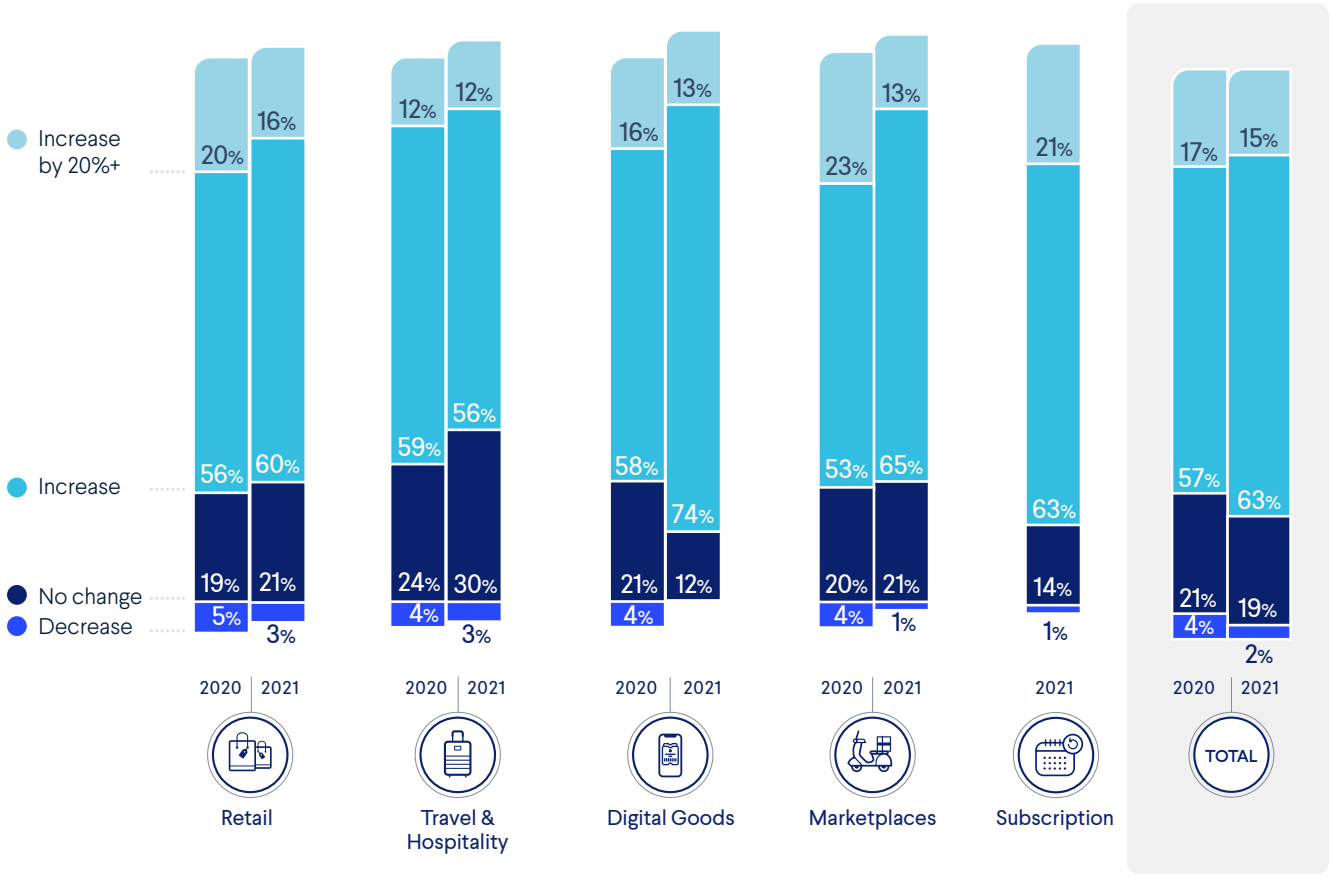
5.0
IS YOUR BUDGET INCREASING IN 2022?

Around 5% more merchants predict that their fraud budget will increase in 2022 than the year before. This isn't a massive difference but it does fit with wider fraud forecasts.

Losses to online payment fraud are set to exceed $25 billion in 2024. Merchants are aware of the growing threat and impact of fraud that comes with the increasing volume of transactions, so are ready to allocate more resources.

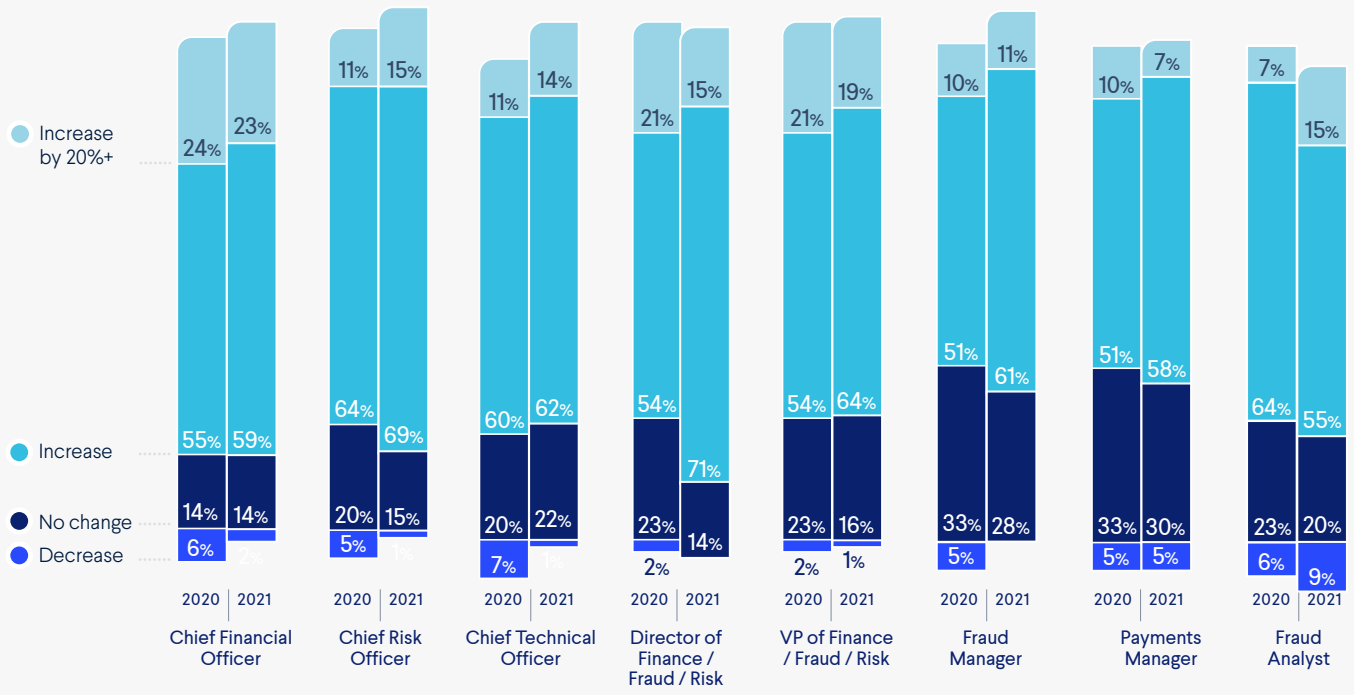
At the same time, fewer merchants believe that budgets will increase by over 20%. This might be because these merchants already have some sort of fraud solution in place and are upgrading rather than starting from scratch. This, of course, will require lower investment.

BUDGET PREDICTION
BY INDUSTRY



5.1 BUDGET PREDICTION BY JOB ROLE

BUDGET PREDICTION
BY JOB ROLE



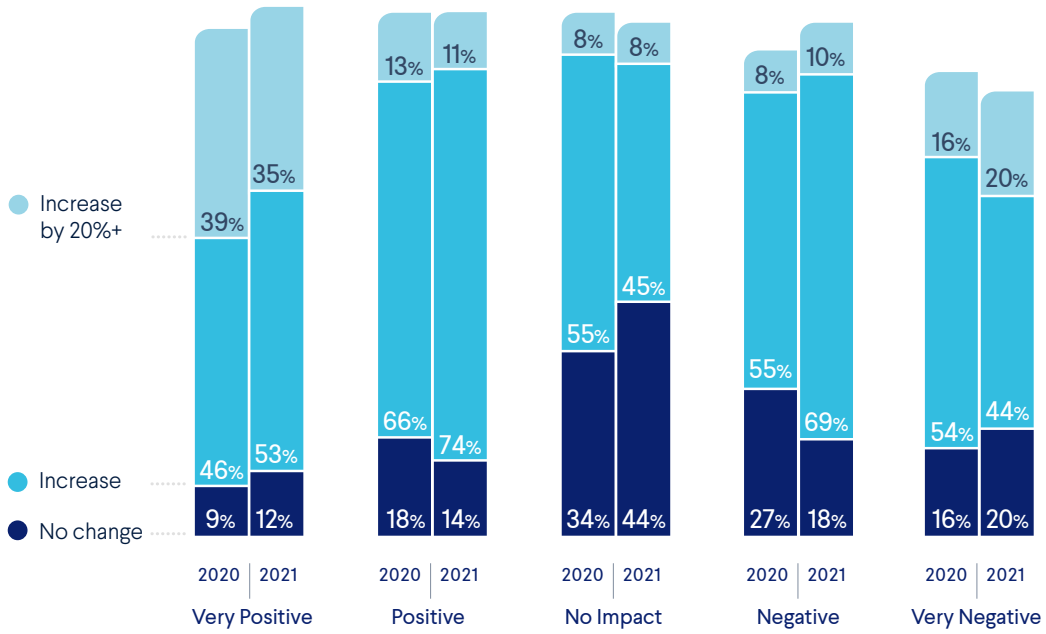
Almost a quarter of CFOs are expecting fraud budgets to increase by over 20% in 2022.

This is really encouraging, as it suggests that focusing on fraud prevention is a top-level priority.

Payment Managers are more optimistic about budgets in 2021 than they were in 2020, but their predictions are still the most conservative. Around 65% of Payment Managers believe that budgets will increase, which is a majority but a smaller proportion than any other role. And 30% predict that budgets will remain the same - the most of any other role. This might be due to a lack of communication from the senior leadership around business priorities or future plans.

5.2 HOW THE PANDEMIC IMPACTS FRAUD BUDGETS

COVID IMPACT ON **BUDGET PREDICTIONS**



We found that merchants who reported that the pandemic had a positive impact on their business were more likely to predict an increase to their budget.

This makes sense, as around half of merchants have seen an increase in order volumes and profits. **By the beginning of 2021**, ecommerce sales hit $4.9 billion. This is set to jump to around $6.4 billion by 2024. Of course, this increase in revenue comes with an increased need to protect it.

Merchants have been forced to quickly adapt and upgrade their online offering to meet increased demand. Unfortunately, fraudsters like to follow the crowd. In light of this, spending on fraud detection and prevention platform services is set to **exceed $11.8 billion globally in 2025**, up from $9.3 billion in 2021.

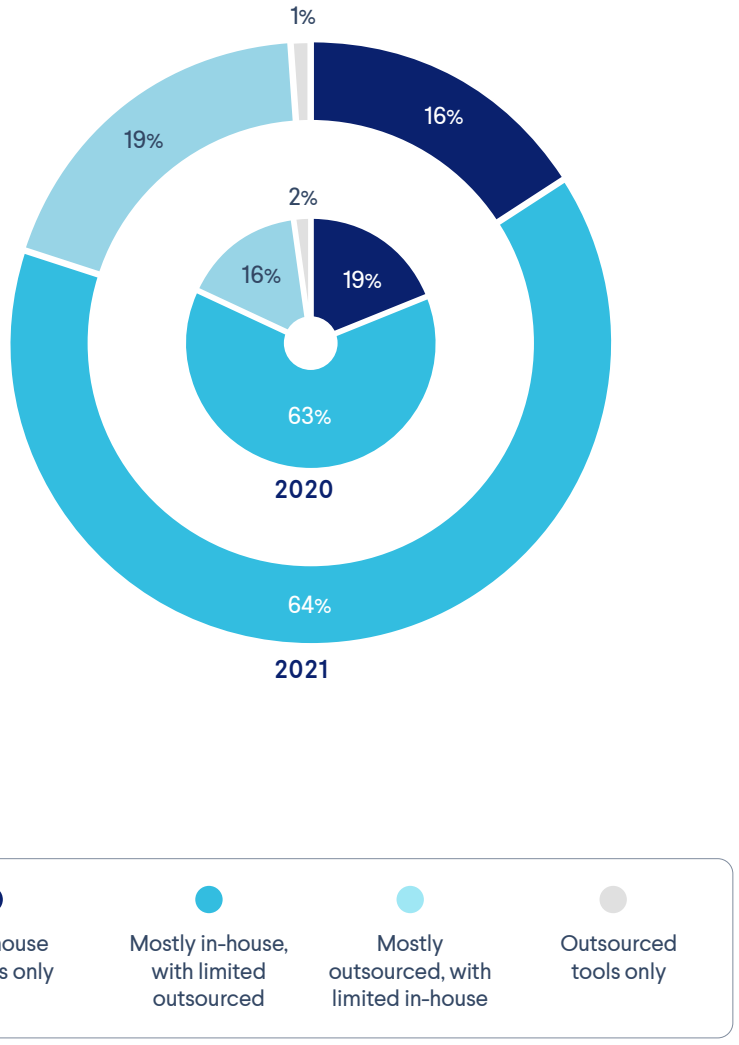
5.3 MERCHANT FRAUD TOOLS BREAKDOWN

Around 83% of merchants use a mix of in-house and outsourced tools, which is up from 2020. Overall there seems to be a shift with less merchants using just in-house tools and more outsourcing the majority.

Why might this be? Many merchants have experienced accelerated growth over the past two years and may have outgrown their in-house tools or the out-of-box solutions provided by payment providers. Handling this increase in transactions is a struggle if you're only working with legacy systems or piecemeal solutions.

Third party vendors allow you to future-proof your security with a fraud solution that scales as your business grows. Outsourced solutions take into account important emerging trends like new payment channels. Your customers also expect a sleeker online shopping experience. So it's vital that your solutions can address issues like friction and false declines.

ARE MERCHANTS USING **IN-HOUSE OR OUTSOURCED TOOLS?**



5.4 FRAUD PREVENTION TOOLS BY INDUSTRY

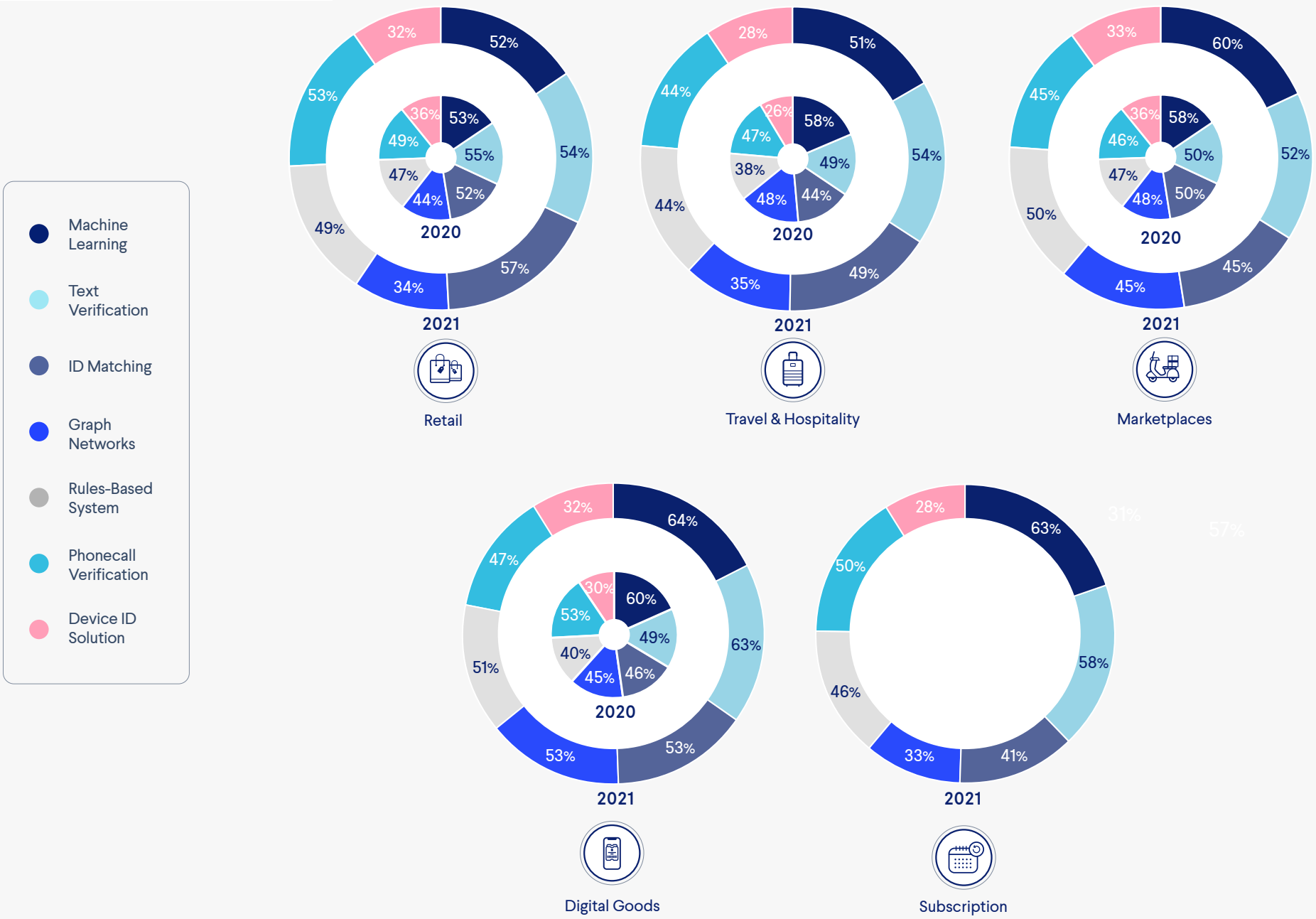
So what specific tools are industries using? It looks like rules are getting more attention – the use of rule-based systems has gone up by 5% across industries.

While this isn't a huge increase, it does suggest that rules are still a relevant part of the prevention toolkit. Why might this be? Rules can act as an immediate first defense in a rapidly-changing environment. So, they've probably been a huge help for many merchants through the pandemic, blocking new types of fraud attacks. This can buy you precious time while you train your machine learning model. That said, relying on rules alone is not a good idea. You need a long-term solution to avoid expanding your rulesets everytime new fraud pops up.

Digital Goods merchants have upped their technology use across the board

This makes sense, as the market has exploded over the last couple of years. Online gaming audiences are projected to surpass 1.3 billion and the market is set to reach **$256.97 billion** by 2025. A similar trend can be seen in the online gambling market, which is anticipated to be valued at more than **$92.9 billion in 2023**. Fraudsters love a booming industry, so Digital Goods teams are having to cover all bases by broadening their toolset.

FRAUD PREVENTION TOOLS **BY INDUSTRY**



6.0
TOP FRAUD RISKS FOR MERCHANTS

What are the top three fraud risks to your business? We asked merchants to rank their biggest threats and here's what they said...

44%
Online payment fraud as no. 1 risk

Online payment fraud and ATO are considered the two biggest risks across all industries, which hasn't changed since 2020. Online payment fraud is the most expensive risk. Global ecommerce losses to online payment fraud hit $20 billion in 2021, a growth of over 14% YoY.

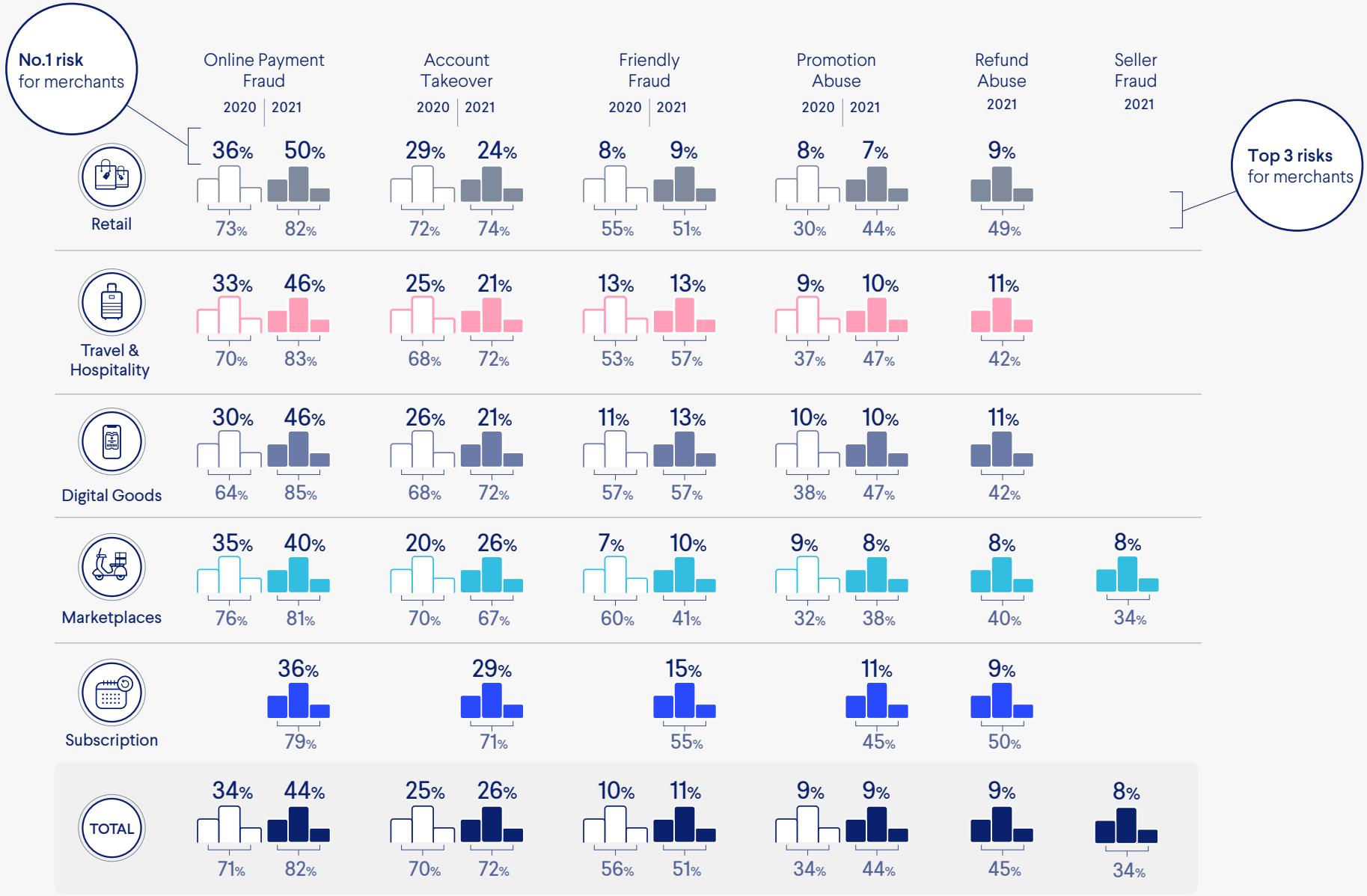
45%
Refund abuse as a top threat

But the fraud risk in third place isn't so clear cut. In 2020, it was friendly fraud. Now friendly fraud is neck-and-neck with promotion and refund abuse. Amid the pandemic more customers are trying their luck at policy abuse. They may be tightening their belts or know they won't get caught. Whatever the reason, the costs of policy abuse can be eye-watering.

34%
Marketplaces see seller fraud as risk

Marketplaces also have the risk of seller fraud, but only 34% of the industry see it as a top concern. Seller fraud (a.k.a. supplier fraud) ranges from low-level policy abuse to sophisticated crime schemes. It can be costly, difficult to prevent and often hard to detect. It could be happening to your marketplace, but you haven't uncovered it yet.

INDUSTRY GROUP PERCEPTIONS OF THE **HIGHEST FRAUD RISKS**

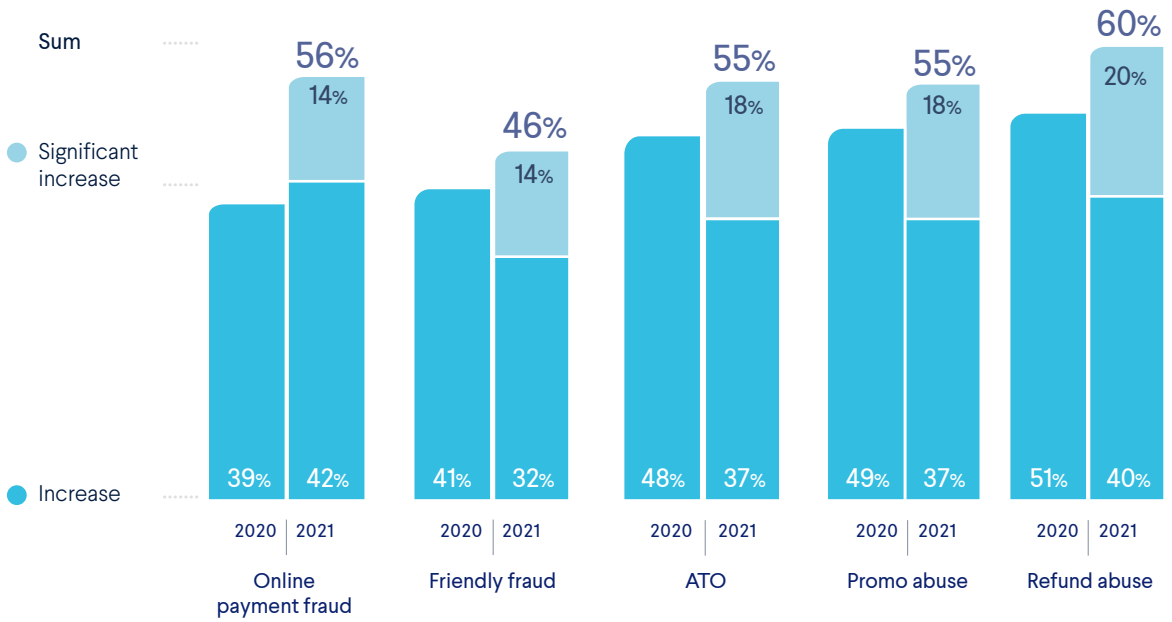


6.1 FRAUD LEVELS OVER THE PAST 12 MONTHS

You may have expected fraud activity would slow down over a year into the pandemic, but the opposite is true. Even more merchants have been affected by growing fraud in 2021 than in 2020.

A huge 20% more businesses noticed an increase in online payment fraud in 2021 than the previous year - the biggest YoY leap. But overall, refund abuse has increased for the highest proportion of merchants, with 20% noting a significant rise.

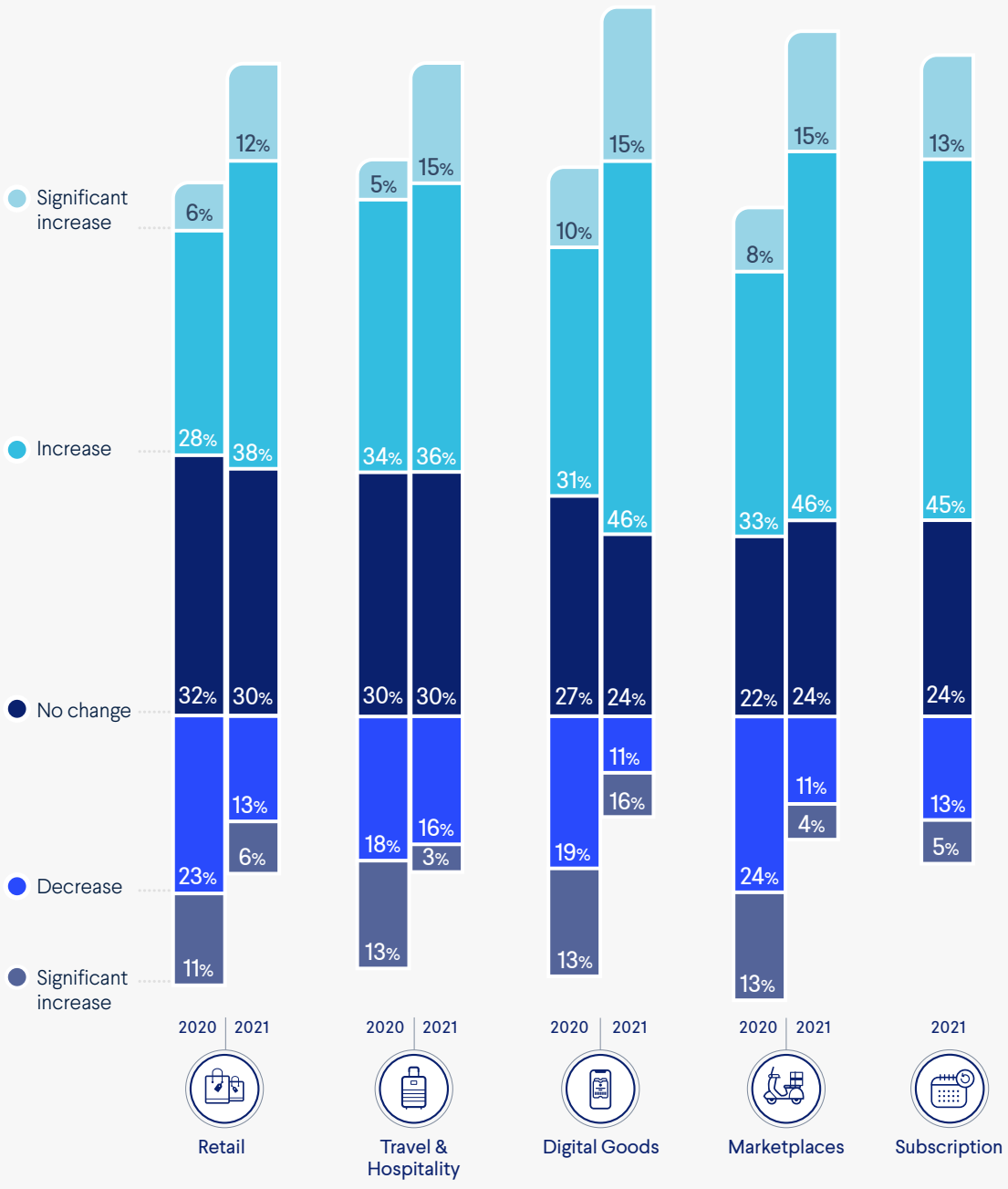
INCREASE IN FRAUD ACTIVITY IN THE **PAST 12 MONTHS**



ONLINE PAYMENT FRAUD
INCREASE IN THE PAST 12 MONTHS

Online payment fraud activity spiked in 2021, as 56% of merchants noticed an increase compared to only 39% in 2020. At the start of the pandemic, around a third of merchants said online payment fraud actually went down. But now, less than 20% of merchants report a decrease.

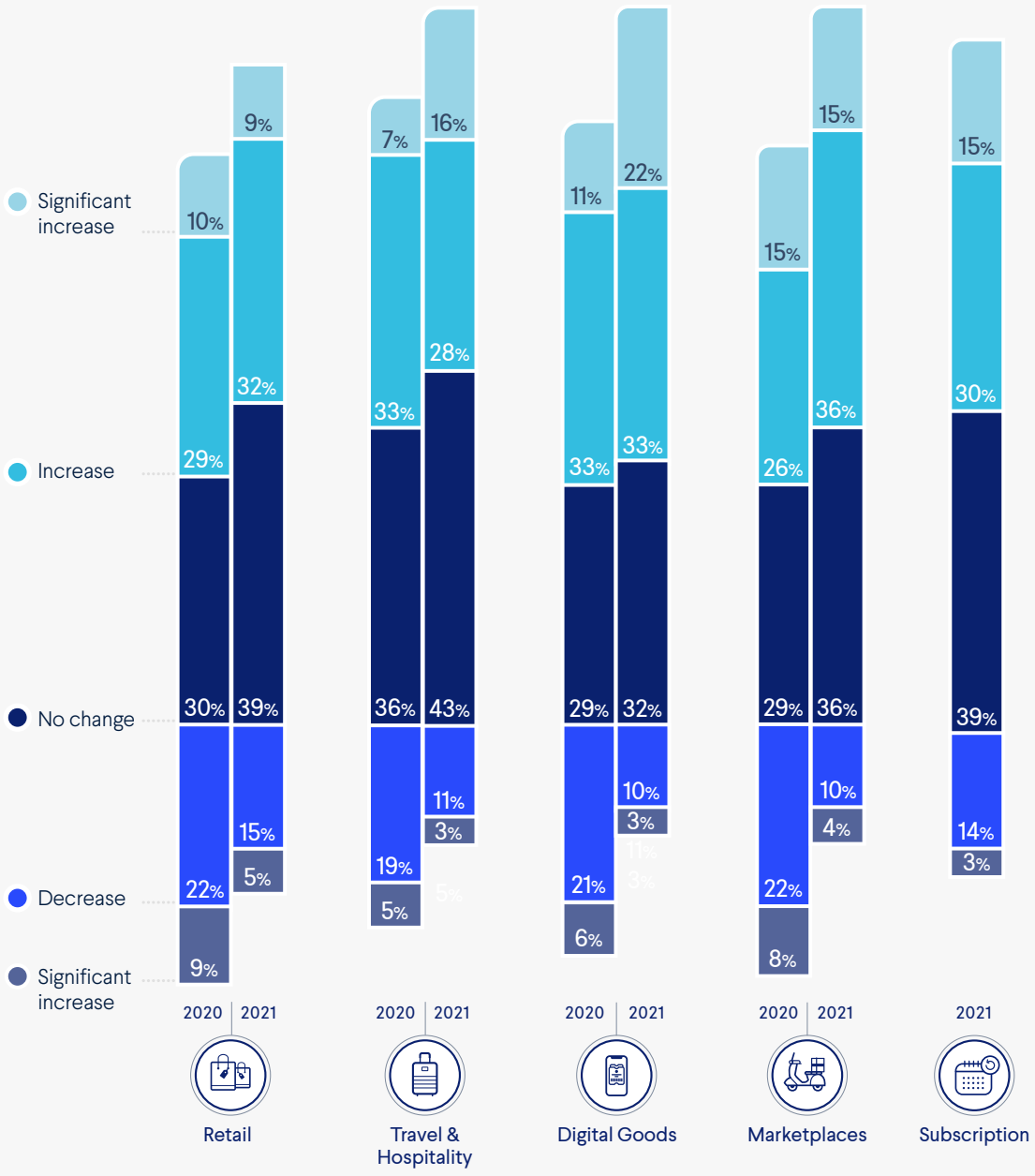
Retailers were most likely to rank online payment fraud as their number one risk, but fewer noticed it increase than other sectors. The threat to retail may not be as fast-growing, but it's still top-of-mind.



FRIENDLY FRAUD
INCREASE IN THE PAST 12 MONTHS

Friendly fraud (a.k.a first-party fraud) involves your customers falsely claiming chargebacks. It's increasing for 46% of merchants, up from 40% in 2020. Digital Goods and Marketplace merchants have been most affected, as over half are seeing a rise.

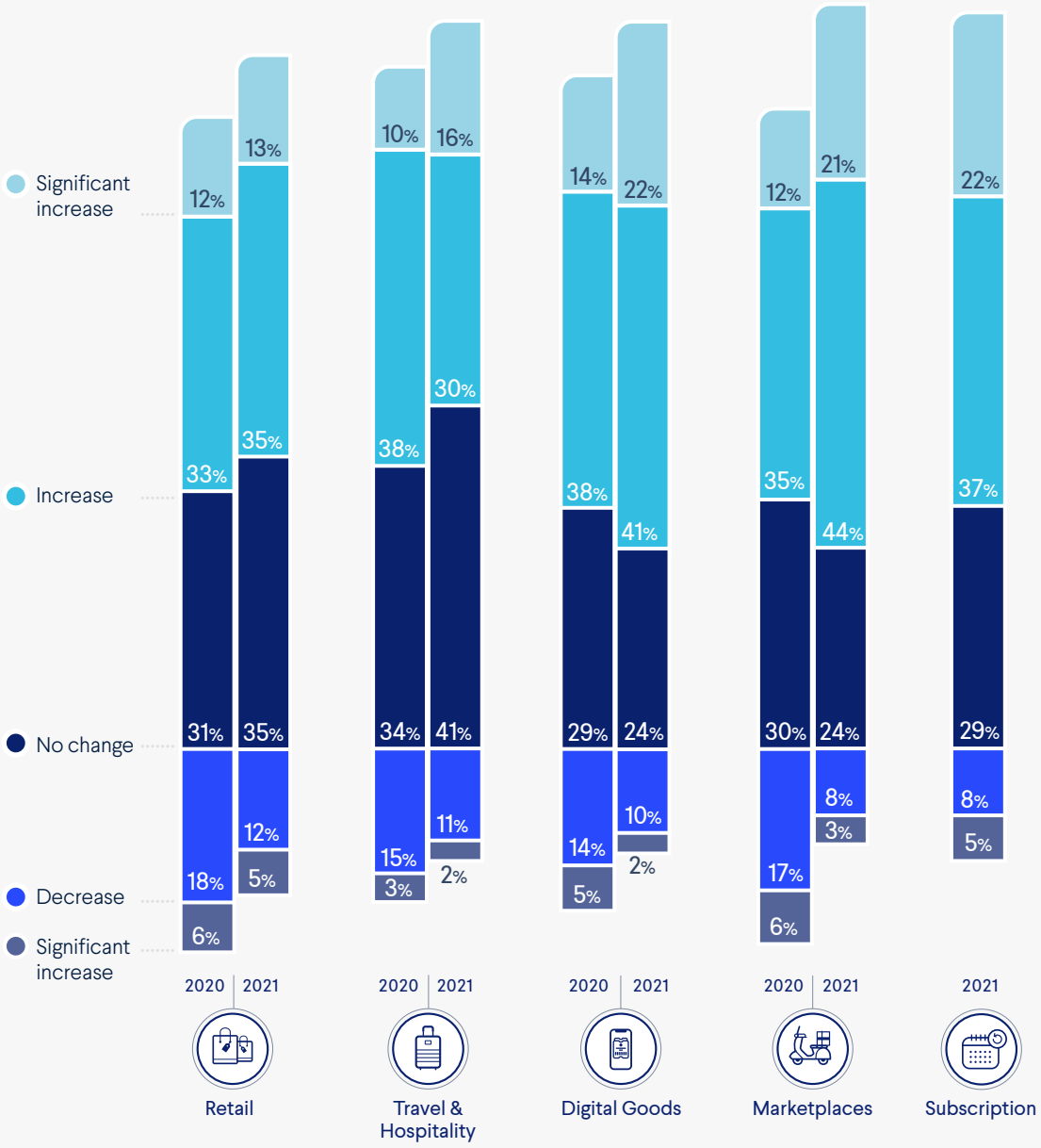
Since the pandemic drove customers online, the new-to-the-internet demographic now comprises roughly **20% of all online shoppers.** This group may be more likely to file an unnecessary chargeback if they are unfamiliar with standard refund processes. If you make your policy terms and conditions clear, you could avoid unnecessary disputes, and even reduce refund abuse.



ACCOUNT TAKEOVER
INCREASE IN THE PAST 12 MONTHS

Account takeover attacks increased for 55% of merchants in 2021, up from 48% in 2020. Almost 20% of all merchants would call the increase 'significant,' and fewer businesses have noticed a decrease in attacks YoY.

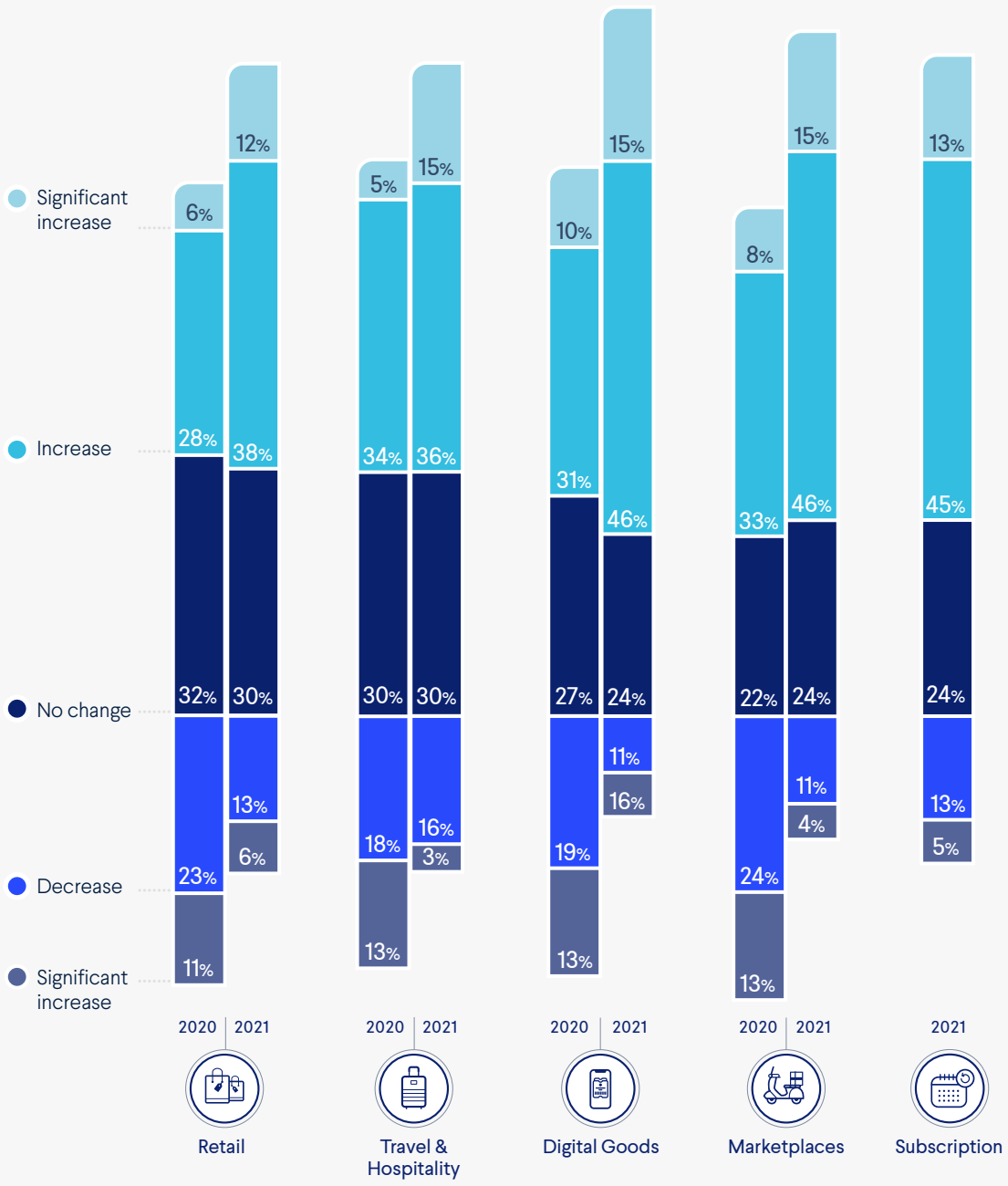
Digital Goods and Marketplace industries have seen account takeover increase more than other sectors. As we will later see, Digital Goods were victim to the most attacks of all industries in 2021, at four high-level incidents per month. Both business types are **easy targets for hackers.** For example, Digital Goods can be easily resold, without operational effort like organizing delivery.



REFUND ABUSE
INCREASE IN THE PAST 12 MONTHS

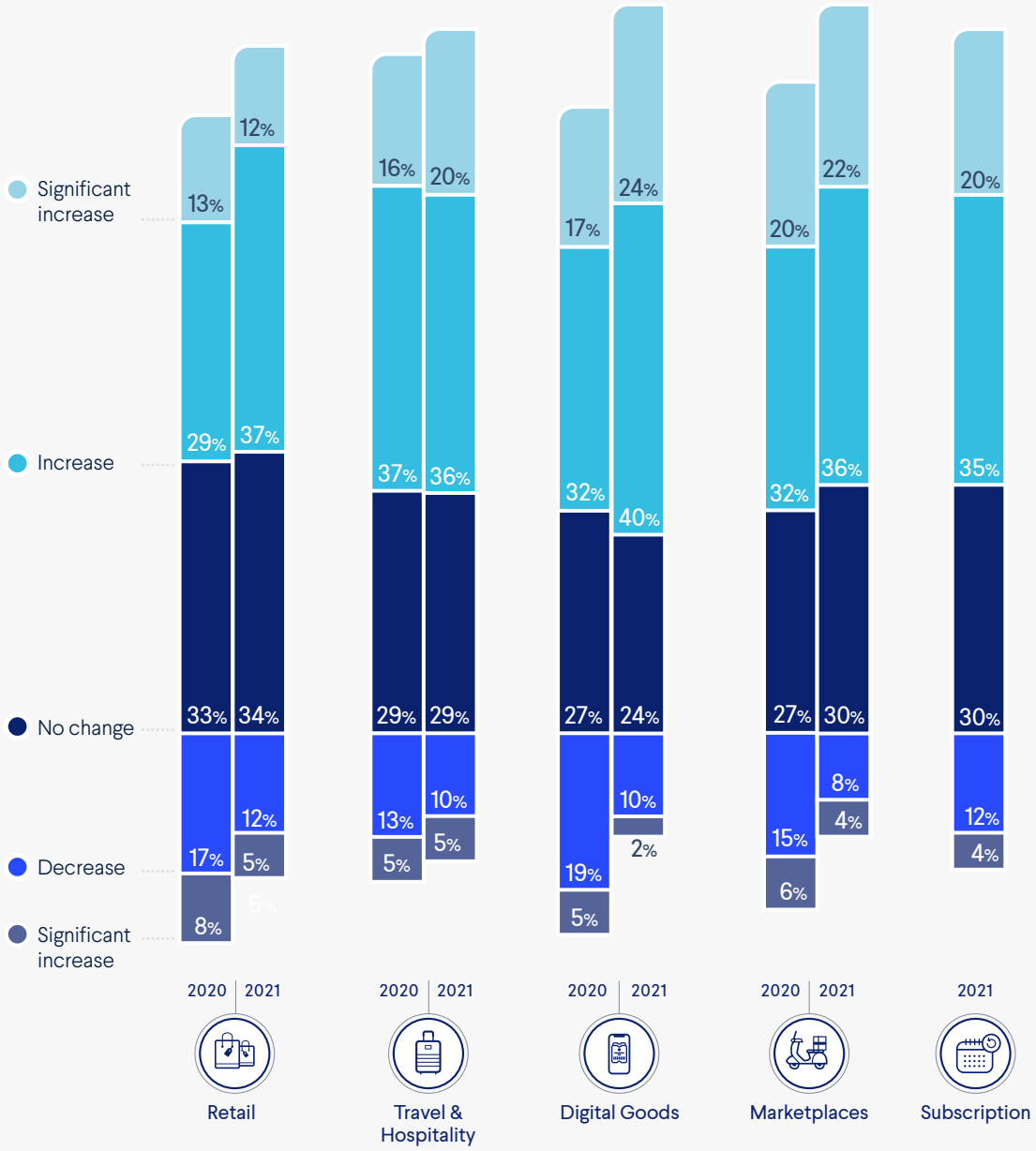
Refund abuse occurs when a customer uses the returns policy of a merchant so much that it becomes unprofitable. Since the start of the pandemic, more merchants are seeing refund abuse rise than any other fraud risk. Covid fulfilment challenges caused genuine refunds to shoot through the roof - unscrupulous refunds could easily slip through the net.

More Digital Goods and Marketplace merchants saw refund abuse rise than other industries. In fact, a quarter of Digital Goods merchants noticed a significant increase. Refund abuse with Digital Goods may not cost you delivery, but it can erode your profits if customers game the system to get your product for free.



PROMOTION ABUSE
INCREASE IN THE PAST 12 MONTHS

Around 55% of merchants saw promo abuse increase in 2021, up from 49% in 2020. Digital Goods merchants saw the biggest change, as 15% more saw a rise over the year. Competition amongst Digital Goods merchants has risen for a quarter of the industry, more than other sectors, so generous marketing schemes can help you stand out! But more promos give your customers greater opportunity to take advantage.



6.2 FACTORS TO IDENTIFY FRAUD

What are your most important factors for identifying fraud? Priorities are different from business to business, but there are some clear trends. Account history and order costs are ranked as most important overall and are in the top three factors for over 70% of merchants.

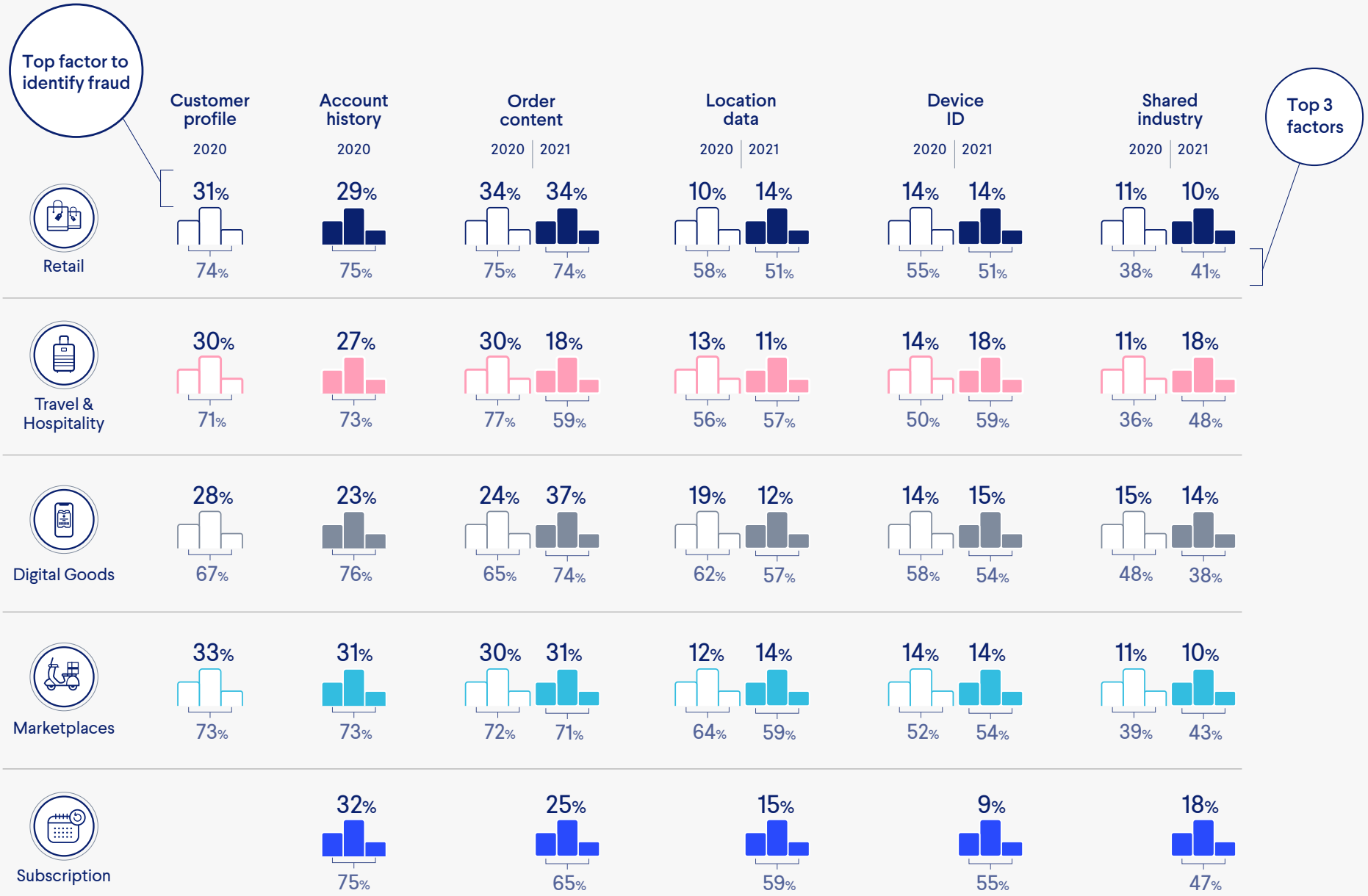
OVER **70%**
account history is a top fraud factor

As you'd expect, trends across industries haven't changed much in a year, but order content has slightly overtaken account history in the rankings. Digital Goods merchants are largely responsible for this shift, as 37% now say order content is their number one factor, up from 24% in 2020.

Shared industry data is still least likely to appear in the top three factors. But it has gained importance for Travel & Hospitality merchants, as the top factor for almost 20%. Travel & Hospitality merchants experience frequent data breach attacks as customer accounts hold valuable credentials, so it's important they're aware of new industry threats.

Overall, every business has slightly different fraud signals. For example, order content will be more important to a retailer than to a subscription business. A one-size-fits-all approach doesn't work - your fraud signals are unique, so you need a bespoke strategy.

FACTORS TO **IDENTIFY FRAUD**

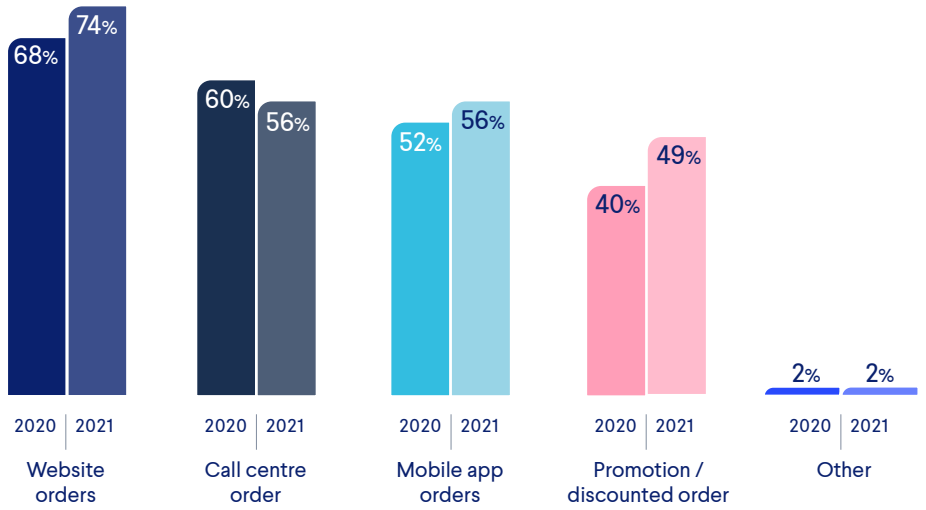


6.3 TRACKING FRAUD BY SPECIFIC DATA

What data do you track for fraud? We asked merchants about which factors are most important. Responses vary depending on what order methods a business offers - if your business doesn't have an app, you can't track app data!

Overall, tracking orders on the web, apps and via discounts increased over the year. Around 74% of merchants track website orders, up from 68% in 2020. Of the companies tracking fraud by promotion, 57% also said they have seen an increase in promotion abuse, suggesting that awareness of policy abuse is growing.

TRACKING FRAUD BY
SPECIFIC DATA



The number of merchants tracking fraud by call centers has reduced since 2020. This is concerning, as **account takeover attacks via call centers are on the rise.** Fraudsters can side-step PDS2 regulations, and target overwhelmed call center staff with phishing techniques. And as call center volumes **rose by up to 800% for some in 2021** it's harder to spot the bad actors. You shouldn't underestimate this risk as it could become your fraud weak spot.

6.4 TRACKING FRAUD BY LOCATION

Fraudsters can focus attacks on merchants in specific countries or regions. So which countries are seeing the biggest increases in fraud?

BRAZIL MEXICO

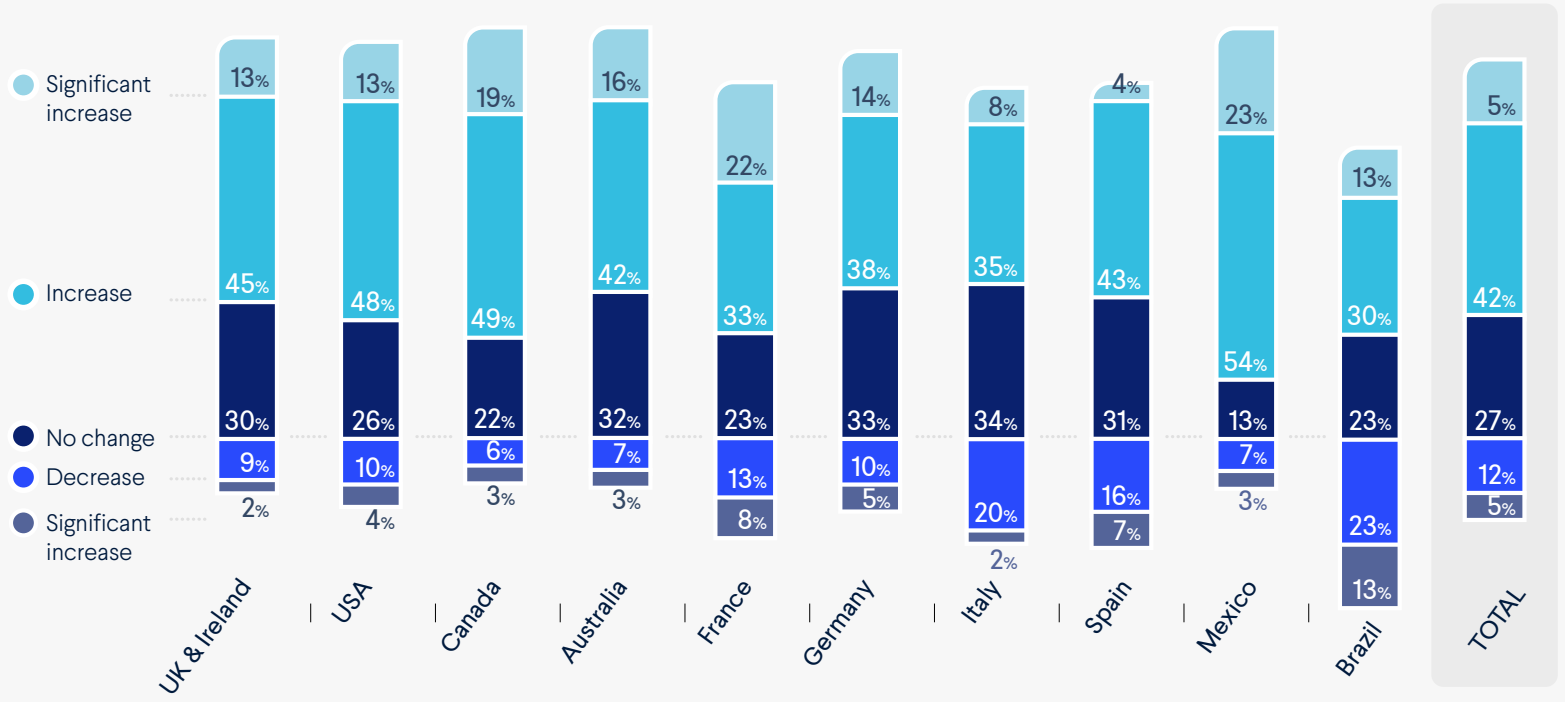
Almost 80% of merchants based in Mexico noticed an increase in online payment fraud in 2021, with almost a quarter saying the increase was significant. Account takeover has also boomed for 70% of Mexico-based merchants. Estimates show that around **20% of new online accounts** created in the region are fraudulent. The pandemic had a massive impact on LatAm payments, as countries like Mexico were previously slower to adapt to digital channels.

In 2018, only **59% of the region had internet-access** and cash was king. When the pandemic hit, digital transactions took off, and the average volume of transactions through online web browsers grew from **26% to 33%.** But there has simultaneously been a huge rise in opportunity for fraudsters, who can focus attacks on the LatAm region from anywhere in the world.

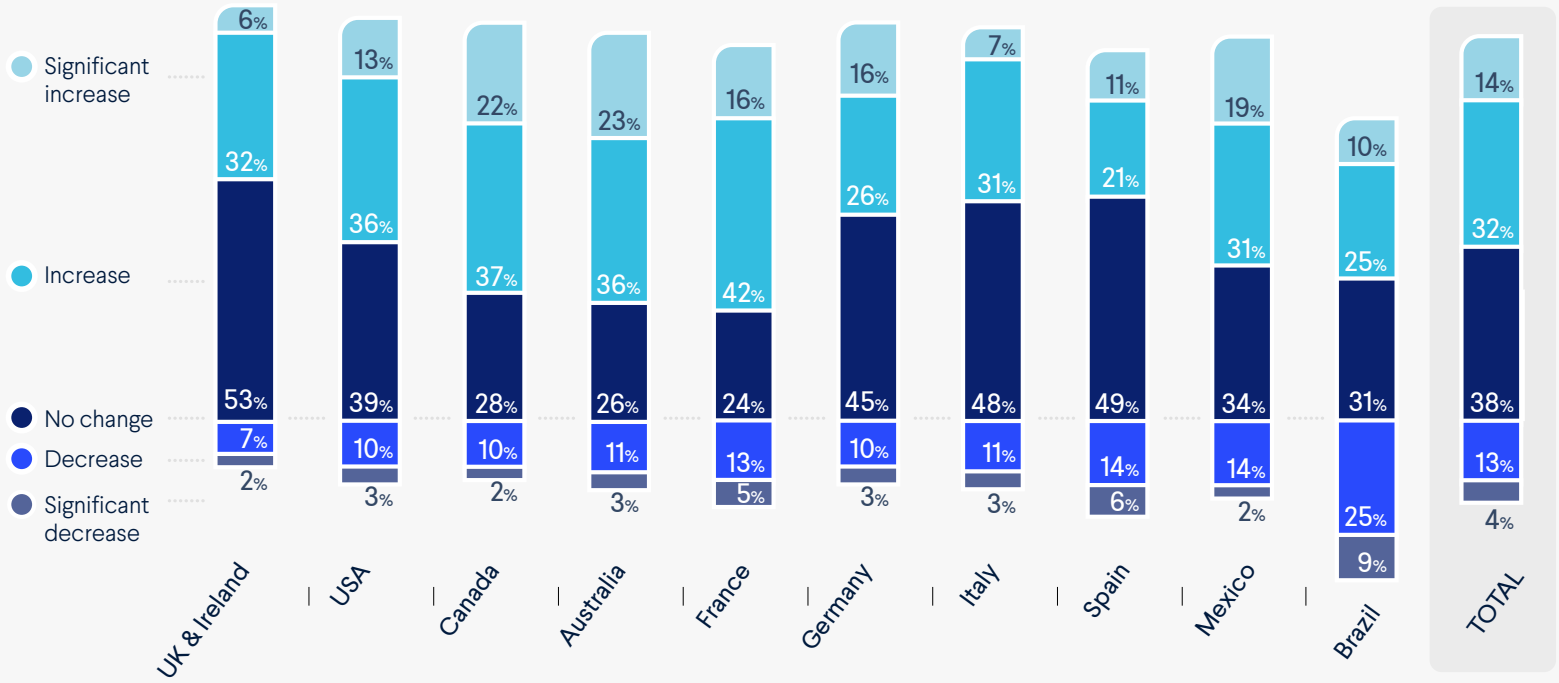
USA

US merchants are seeing fraud of all types rise at a faster rate than those in the UK or Europe. For example, 61% of US merchants have seen an increase in online payment fraud, compared to only 49% in Europe and 58% in the UK.

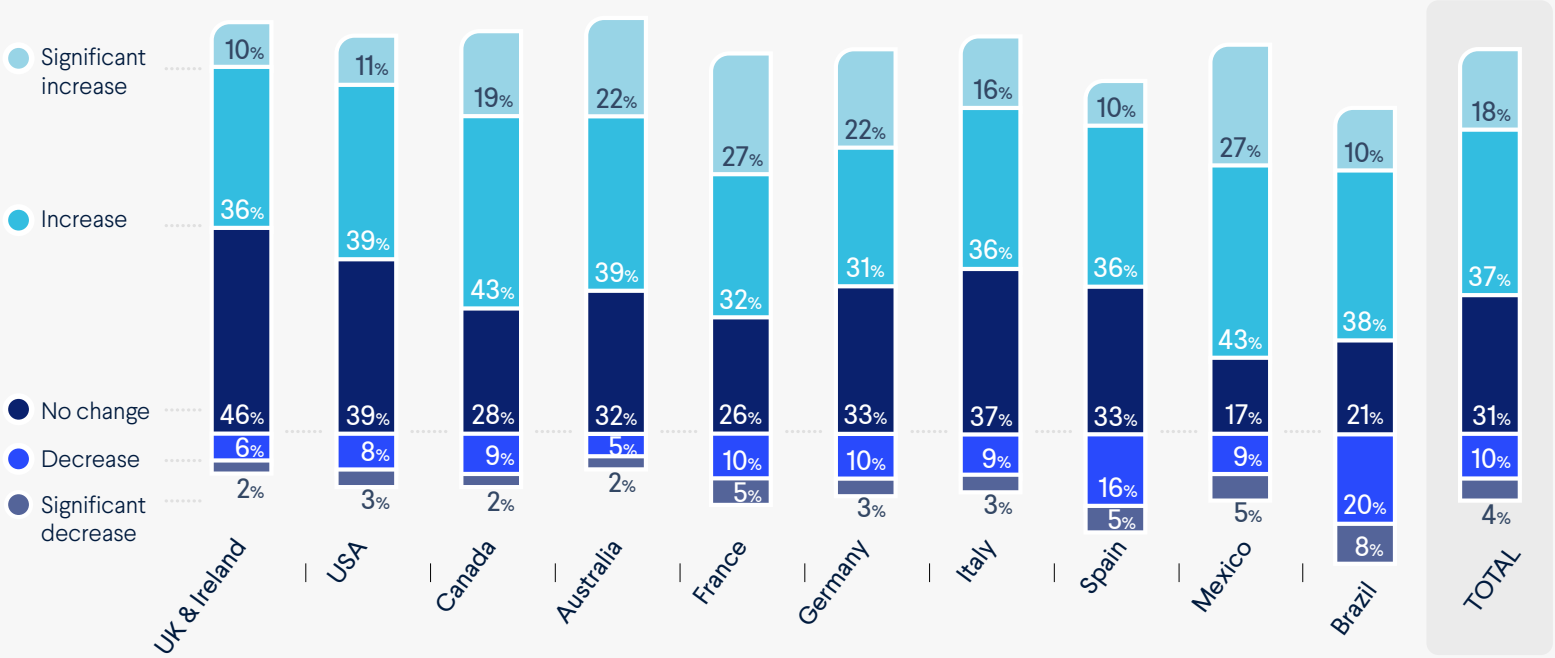
TRACKING ONLINE PAYMENT FRAUD BY LOCATION



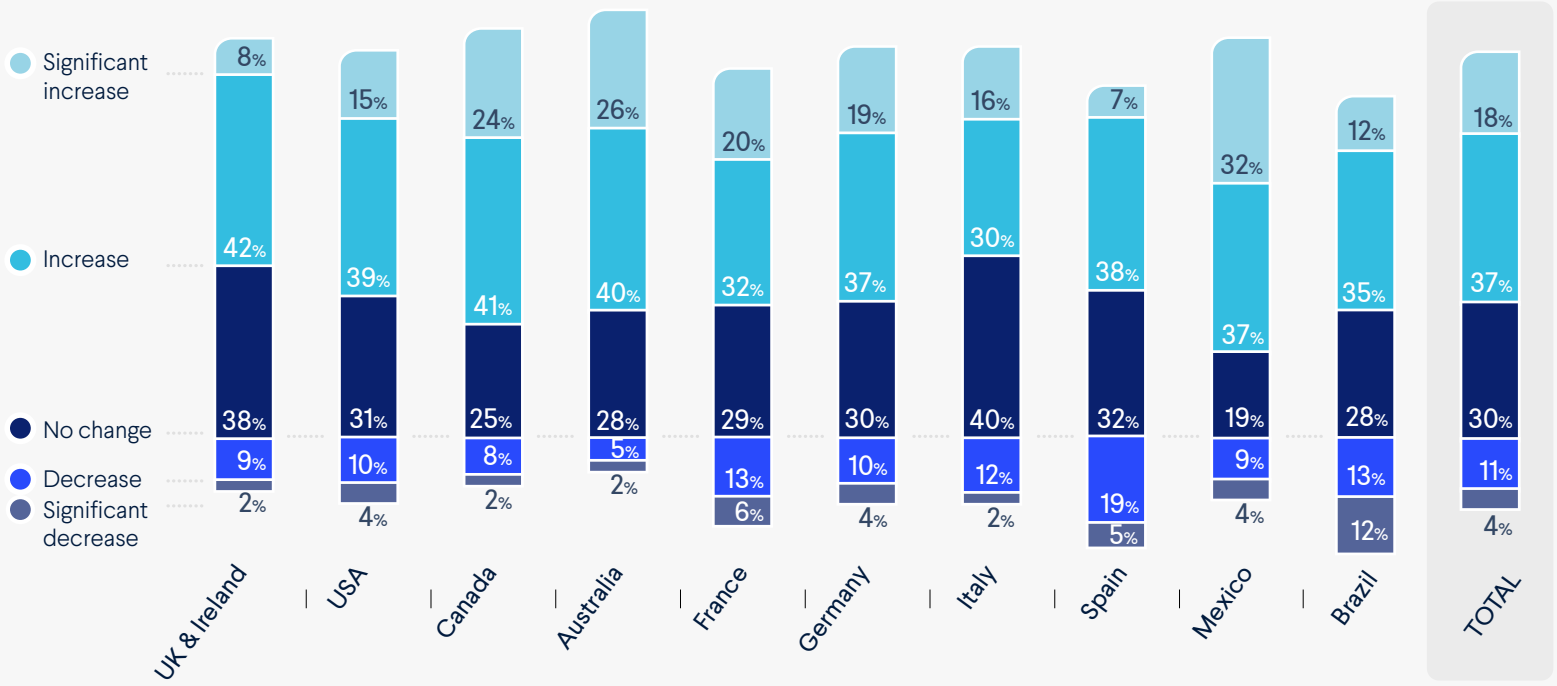
TRACKING FRIENDLY FRAUD
BY LOCATION



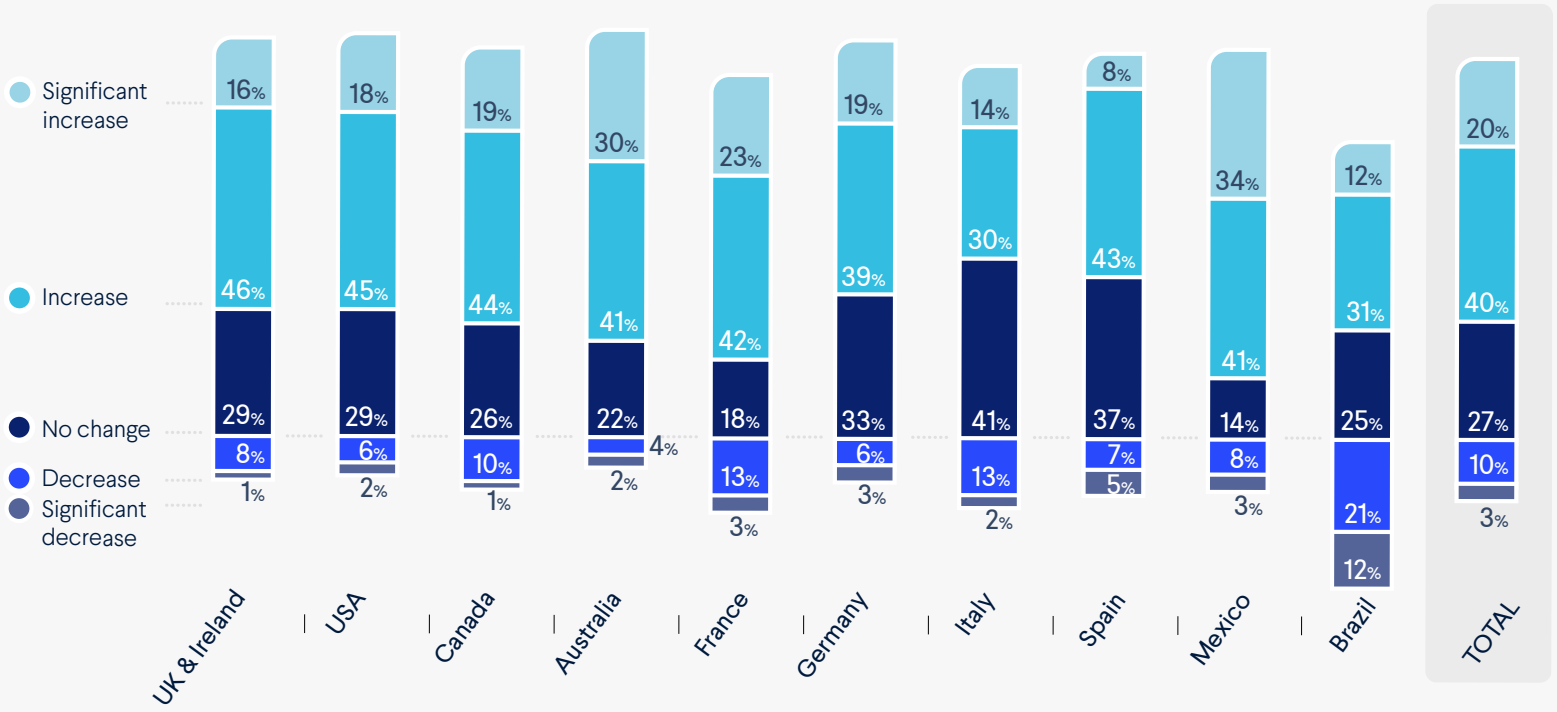
TRACKING ACCOUNT TAKEOVER FRAUD BY LOCATION



TRACKING PROMO ABUSE
BY LOCATION



TRACKING REFUND ABUSE
BY LOCATION

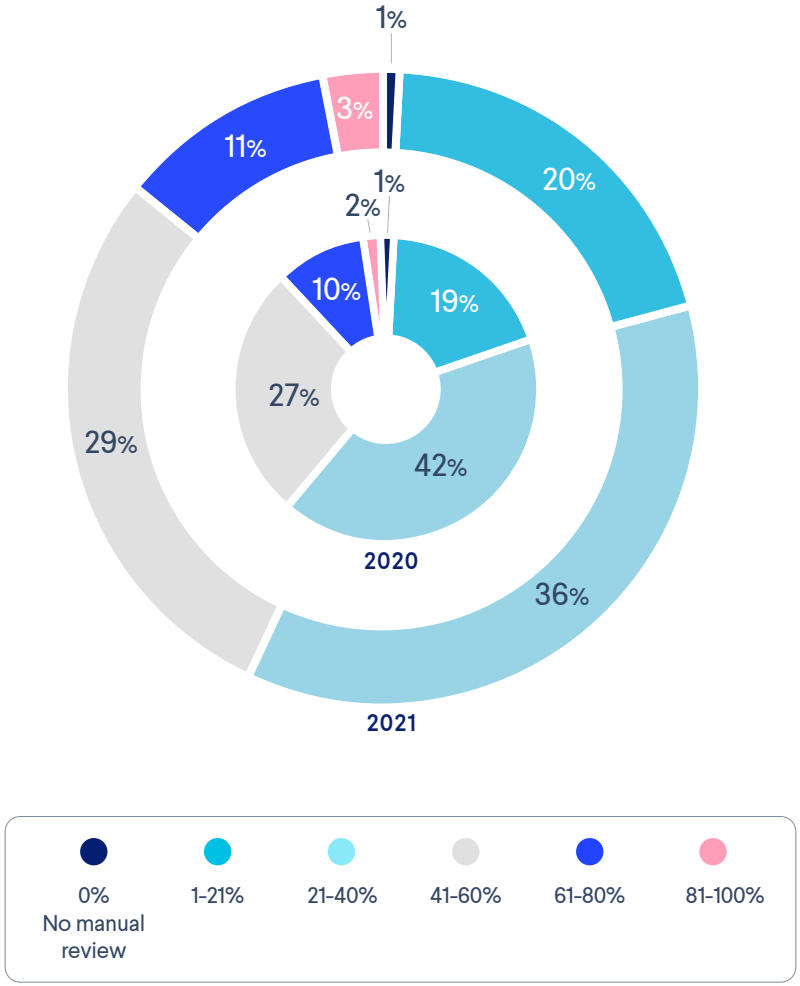


7.0 TIME SPENT ON MANUAL REVIEW

With all these new technologies, we wanted to find out if there's still a place for manual review. Over two-thirds of merchants spend 20-60% of their time on manual review, which hasn't changed since 2020. So evidently there is! Only 1% of merchants do none at all.

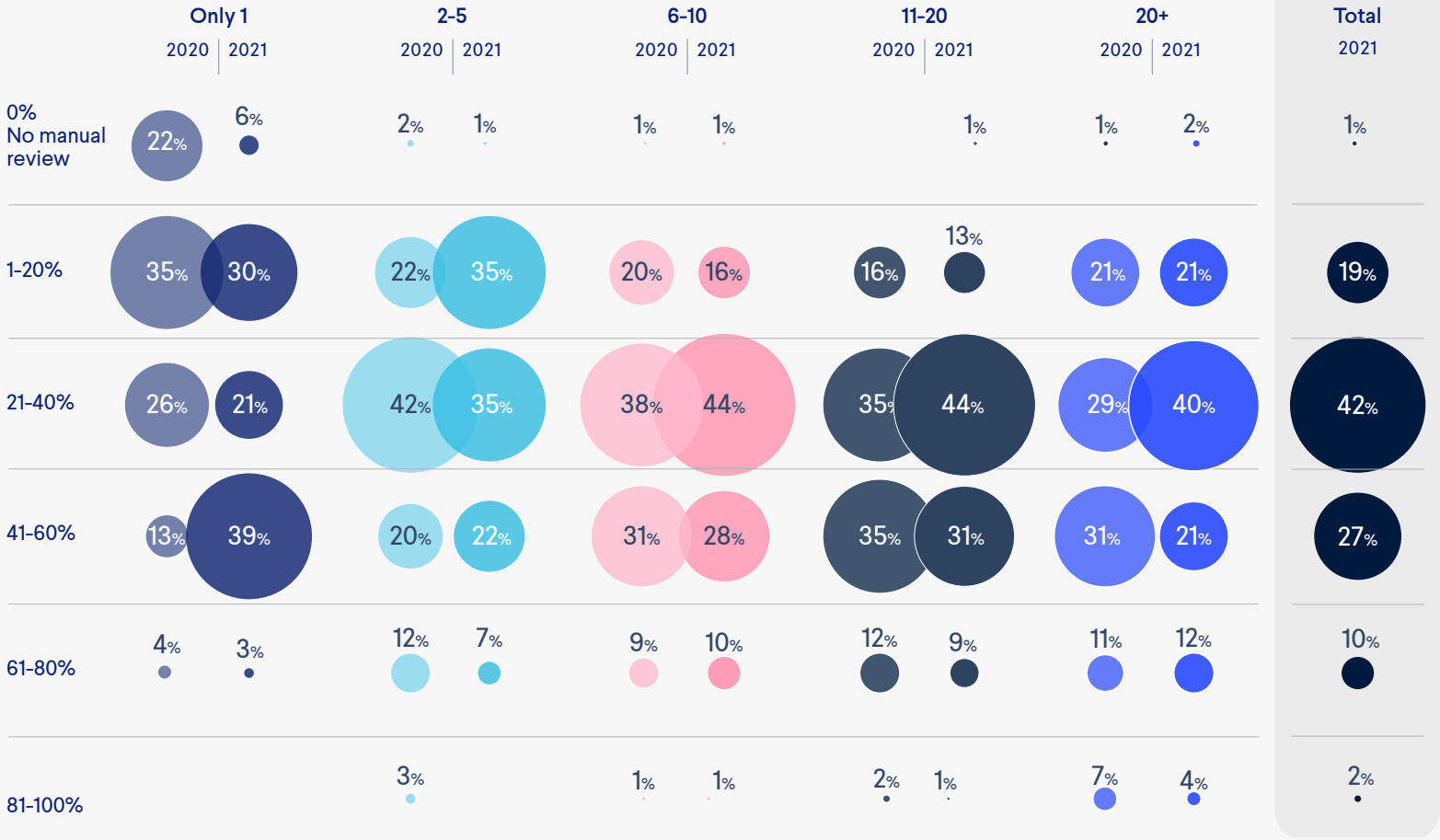
That said, only 2% of merchants spend over 80% of their time on manual review. This low number is likely due to the fact that manual review is time intensive. But occasionally a transaction will pop up that may be worth an additional review. This is the case for transactions that are flagged as risky but may actually be legit.

TIME SPENT ON MANUAL REVIEW



7.1 EVEN LARGE TEAMS INVEST IN MANUAL REVIEW

TIME SPENT ON MAUAL REVIEW **BY TEAM SIZE**

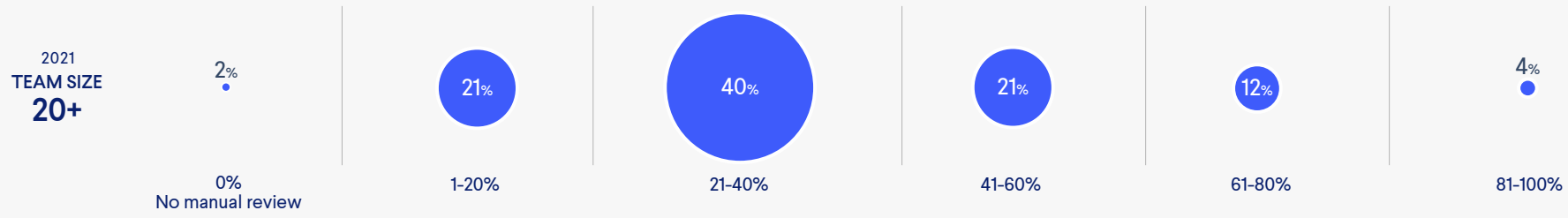


A good fraud strategy is about balancing your block rate and acceptance rate to maximize revenue and minimize risk. You don't want to block legitimate customers, but you don't want to make your business an easy target for fraudsters. Manual review is great for transactions that fall into this gray area.

This is likely why we are seeing that even bigger teams dedicate substantial time to manual review. In fact, 16% of teams of over 20 spend over 60% of their time on manual review. With more resources, they can probably afford to invest in technology. So it goes to show – human insight is still valuable! You really can't replace the insight that an expert human being is able to provide when a questionable order pops up.

Does this mean that we shouldn't invest in tools? Of course not! Technology makes our lives easier and allows us to be reactive, proactive, and better still – predictive. When it comes to manual review, tools can help enhance this critical activity. Good tools are about making manual review more effective, tasks more impactful, and analysts' lives easier - not trying to replace those analysts.

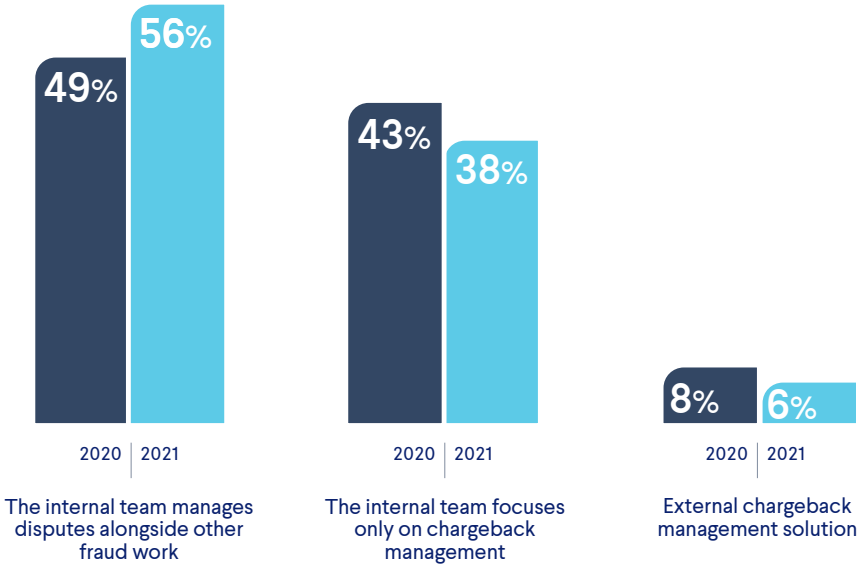
TIME SPENT ON MAUAL REVIEW **BYTEAM SIZE 20+**



8.0 DISPUTE MANAGEMENT OPERATIONS

In 2021, more merchant teams are managing disputes alongside other fraud work, and slightly less have internal dedicated dispute teams than in 2020. This could be because the ecommerce boom caused workloads to rise generally, so merchants have more to juggle.

DISPUTE MANAGEMENT OPERATIONS



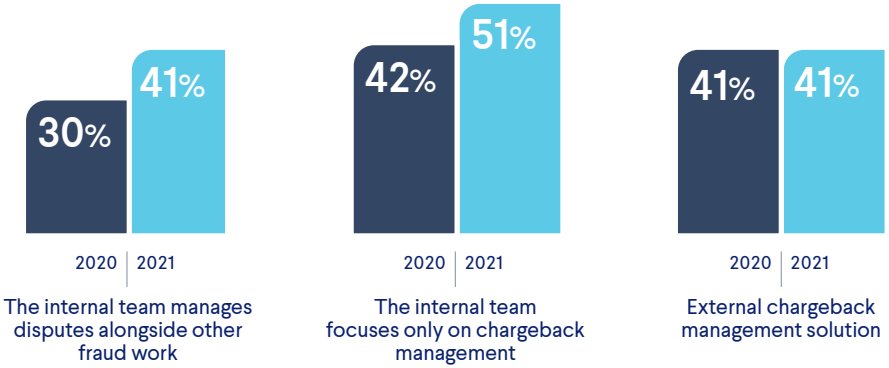
In 2020, on average, companies challenged 37% of chargebacks, and were successful in 56% of challenges. In 2021, companies challenged 48% of disputes, and were successful in 66% of challenges. Challenge to success rate is similar YoY but overall companies challenged more disputes in 2021.

Merchants may have been receiving more friendly fraud chargebacks in 2021. Or since many businesses have recently invested in fraud budgets and hiring, now more teams may have greater capacity to focus on disputes.

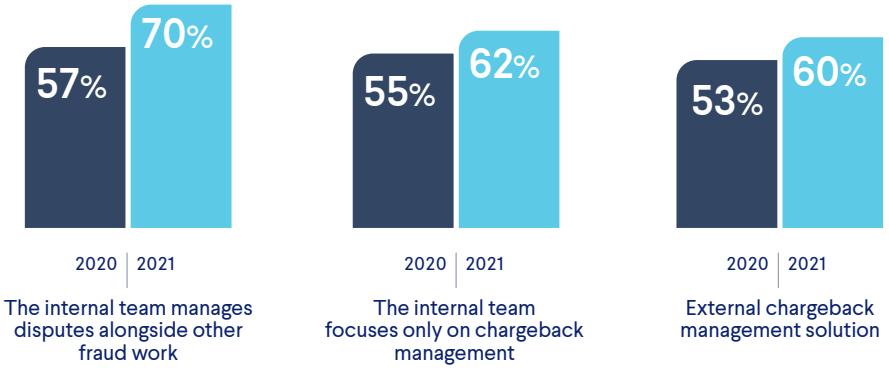
8.1 DISPUTE CHALLENGE SUCCESS

Who handles disputes in your business? In 2020, companies with a dedicated dispute team, internal or external, challenged more chargebacks than those without a dedicated team. In 2021, those with an internal team focused only on dispute management challenged the most disputes of all.

DISPUTE METHOD AND CHALLENGE RATE



CHALLENGE SUCCESS RATE AND DISPUTE METHOD



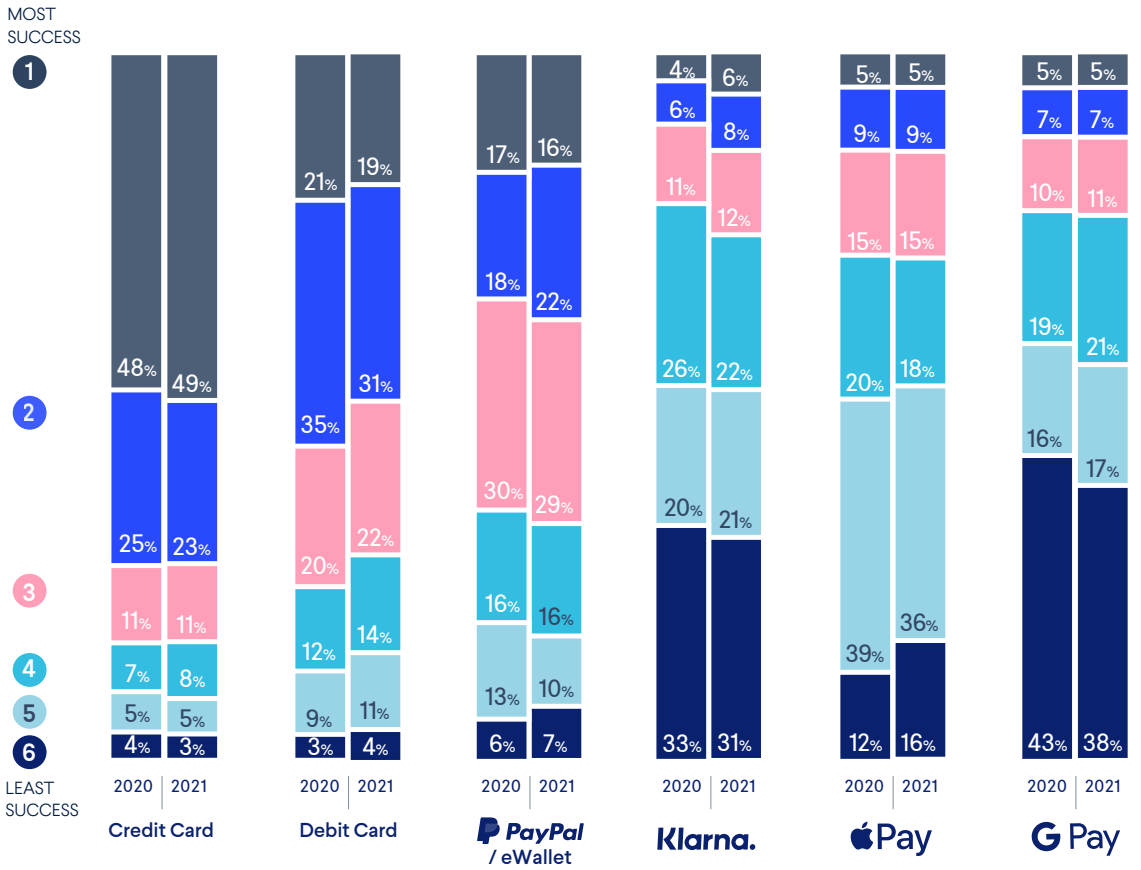
Regardless of approach, chargeback dispute success rates were higher in 2021 than 2020 overall. This could be in part due to regulation changes, as **Visa updated their chargeback rules in October 2021** in response to mounting chargebacks caused by the Covid-19 crisis. The changes were intended to reduce chargebacks and give merchants more opportunity to reduce dispute issuances.

But, internal teams managing disputes alongside other fraud work seem to have a higher challenge success rate. This is perhaps because they have other priorities so challenge less disputes than the dedicated teams, and will only challenge disputes they are sure to win.

8.2 DISPUTE CHALLENGE SUCCESS BY PAYMENT METHOD

Merchants consistently see the most success when challenging credit and debit card disputes. Newer payment methods cause merchants the most trouble, as challenges on GooglePay and Klarna are most difficult to win. This is because customer payment information is obscured, so merchants often don't have the evidence they need.

CHALLENGING DISPUTES SUCCESS
BY PAYMENT METHOD



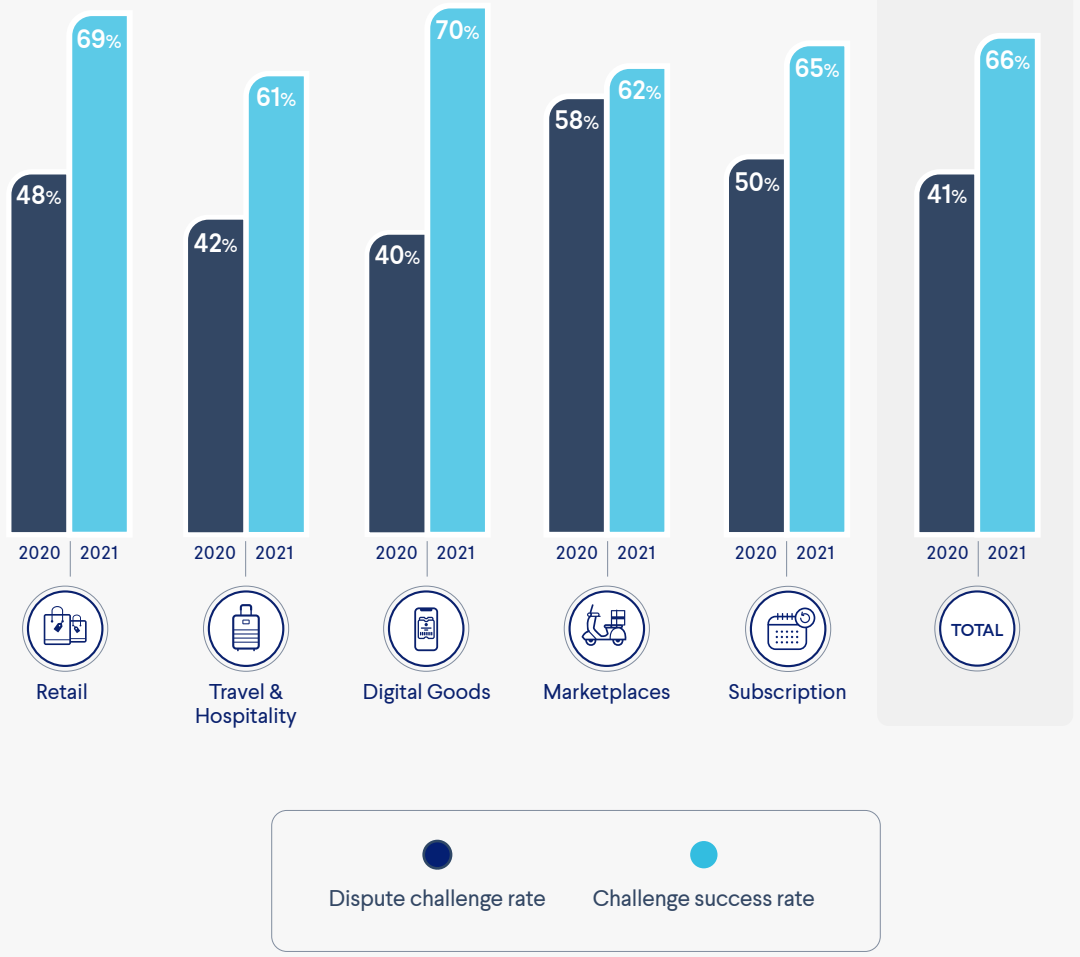
This is becoming increasingly frustrating for fraud teams as the popularity of BNPL and digital wallets is rising. Globally, the use of BNPL during Cyber Week **jumped 29% YoY**. And **32% of mobile wallet users** now have three or more wallets on their smartphones, up from just 21% a year ago.

8.3 DISPUTE CHALLENGE SUCCESS BY INDUSTRY

Travel & Hospitality merchants challenge the least disputes at 40%, and have the lowest success rate at 61%. This is likely because of the record-breaking number of genuine disputes filed during the pandemic due to global travel restrictions.

Nearly **one-third of the US population** booked hotel rooms or reserved tickets for attractions/ events in 2021. **More than half of this group, 60 million people,** canceled their reservations, and most of them wanted their money back. If your customers couldn't get a refund, they would've contacted their bank.

CHALLENGE SUCCESS
BY INDUSTRY



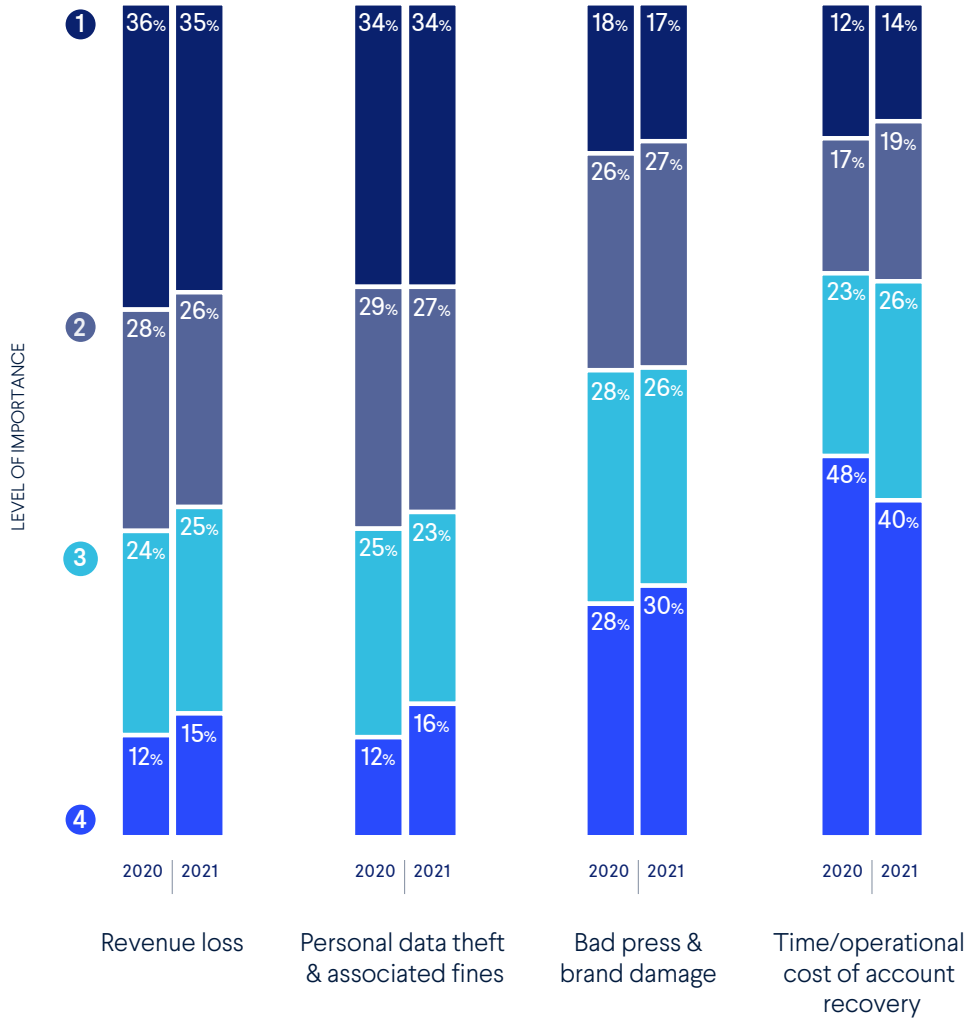
9.0 ACCOUNT TAKEOVER

Account takeover is one of the fastest growing forms of fraud - almost 60% of merchants have seen an increase in attacks. We asked these merchants which risks associated with account takeover they were most concerned about.

With losses of up to **$26 billion in 2020** alone, it's no surprise that revenue loss is the leading risk for merchants when it comes to ATO – 35% put it as number one. That said, account takeover not only impacts your bottom line but your relationship with customers. But our results show that this is viewed as a lesser risk. Only 17% of merchants see this as the most important threat to their business.

Customer and brand loyalty are directly linked to retention, so why aren't merchants worried? The consequences of brand damage are not as obvious as immediate financial risks, like revenue loss and associated fines. For example, **UK and EU GDPR and Data Protection Act fines** can reach a whopping £17.5 million (€20 million) or 4% of annual global turnover! Also, bad press might be seen as a marketing and PR issue and not one for the fraud team.

ACCOUNT TAKEOVER
RISKS RANKING



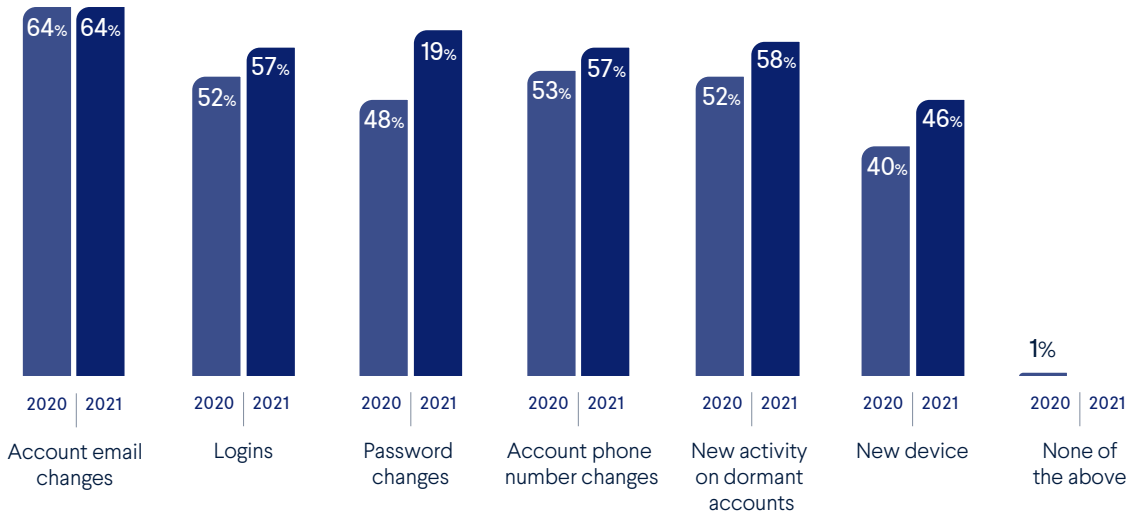
9.1 ACCOUNT ACTIVITY TRACKING

There isn't a significant difference in the tracking activities of merchants that use account takeover tools and those that don't. Account email changes are the most commonly tracked activity over the last two years. Around two-thirds of merchants both with and without account takeover tools reported tracking this activity.

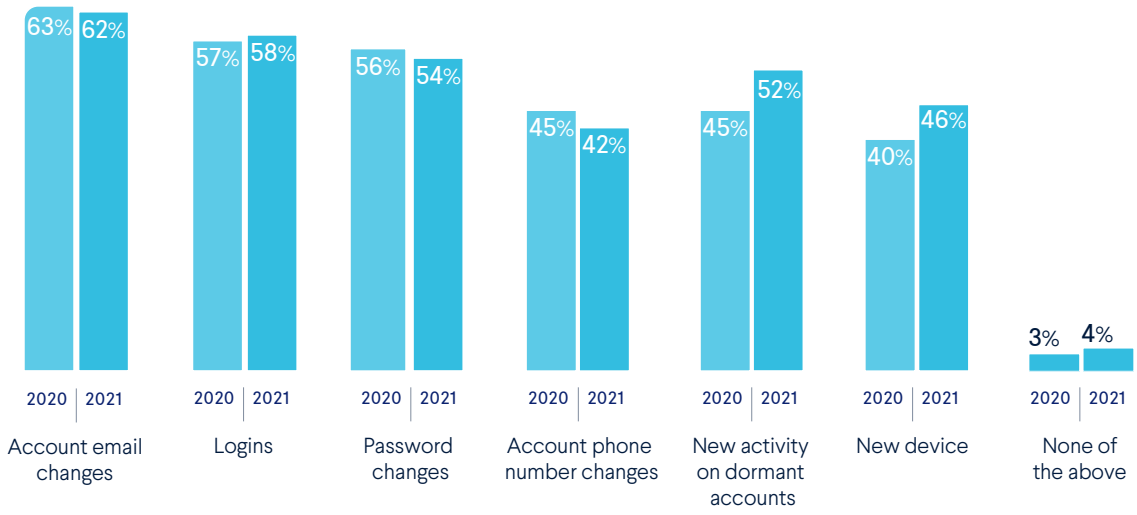
Our analysis has shown that attackers are more likely to change the phone number on the compromised account than the email address. And, in around 15% of attacks, the phone number on the account was changed twice or more. But only half of our respondents say that they track this activity. For the other half, this is a huge vulnerability.

ACTIVITY TRACKING

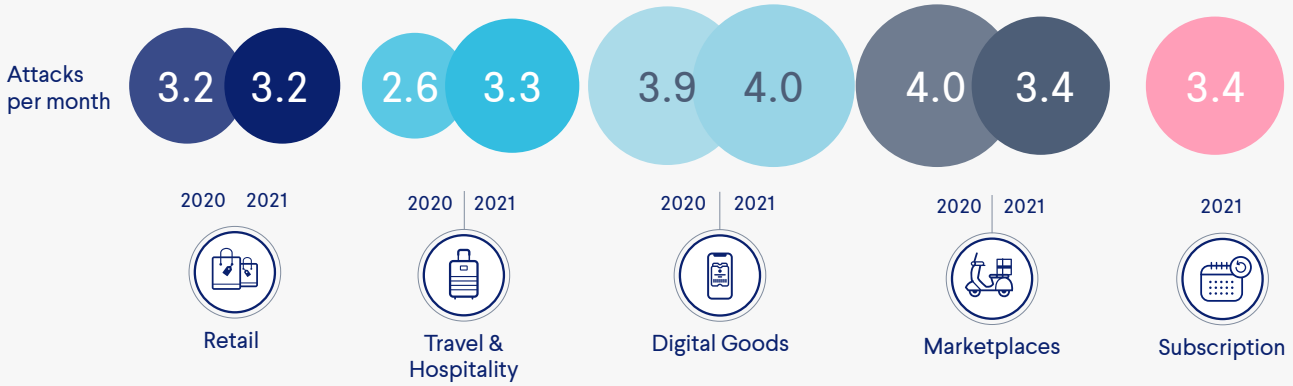
With ATO Tools



Without ATO Tools



9.2 ACCOUNT TAKEOVER ATTACKS IN THE PAST YEAR



We asked merchants about the number of high-impact account takeover attacks they see in a year. These attacks are classified as impacting a large percentage of users and having a significant impact on operations.

Account takeover attacks have increased across the board. The Travel & Hospitality sector has seen the biggest increase in attacks since last year with an average of 39 attacks a year - that's 3.3 a month, up from 2.6 in 2020. This sector has always been a prime target for account takeover attacks due to the amount of sensitive data that merchants need to collect from customers. Accounts also give fraudsters access to valuable loyalty points and frequent flyer miles.

Travel loyalty account takeover is not a new problem. An estimated 14 trillion frequent flyer miles and hotel points go unused each year. But this has been exacerbated by the pandemic travel restrictions, which has left many accounts dormant and unmonitored. One study found that the top five most valuable airline loyalty programs in the US ended 2020 with a combined balance of $27.5 billion in unused loyalty program miles. This is a goldmine for fraudsters, who can easily transfer the points to make high value purchases.

Digital Goods merchants experienced the most attacks in 2021 with four attacks a month, overtaking marketplaces. Pre-pandemic, there were already reports of us entering the "Digital Goods Age" and Covid-19 has massively accelerated this. Fraudsters have been having a field day with this unprecedented volume of new accounts.

39
attacks per year in the Travel & Hospitality sector

9.4 REPORTING OF ACCOUNT TAKEOVER ATTACKS BY COUNTRY

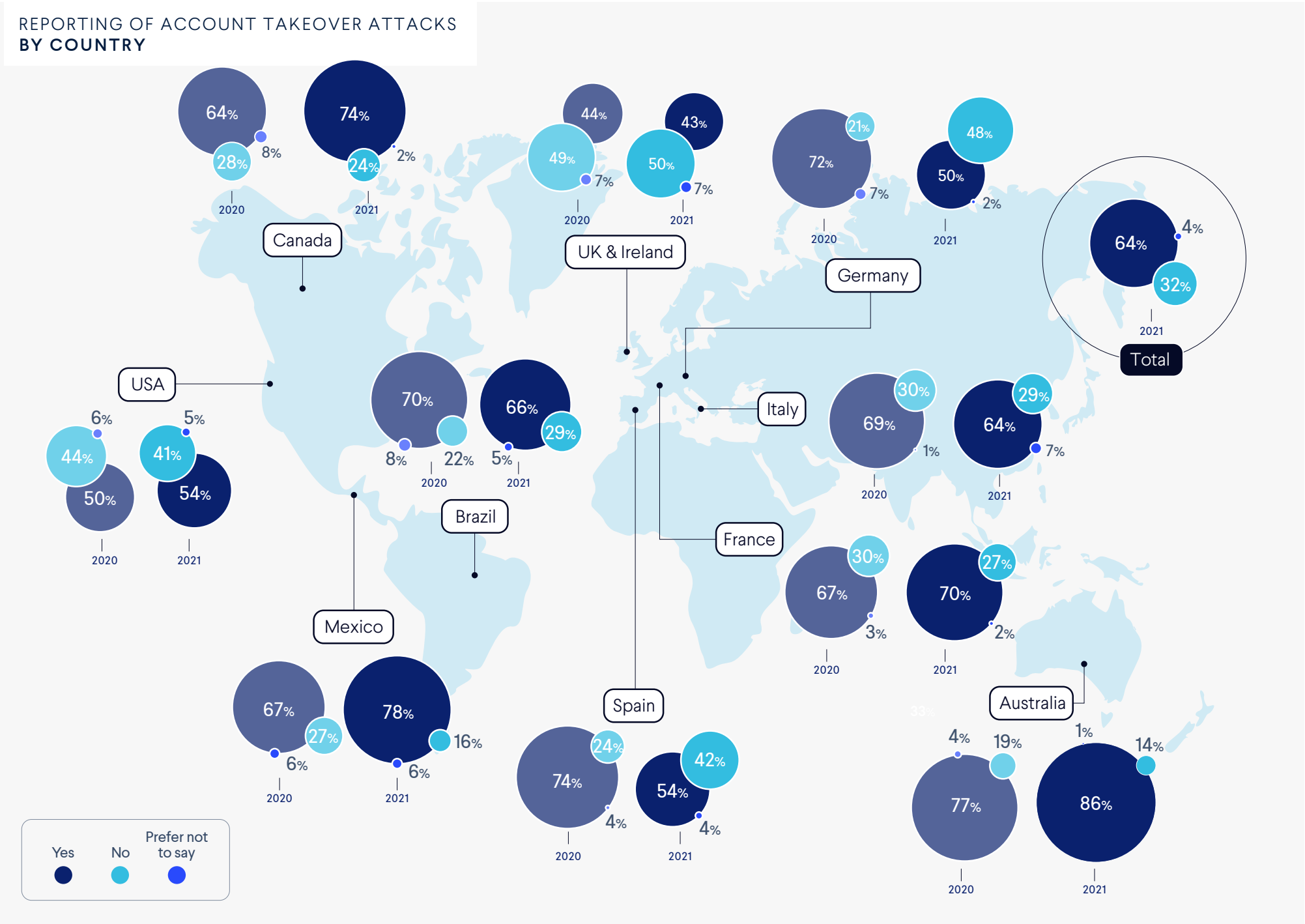
Overall the majority of merchants across regions did report account takeover attacks this year. But we can't overlook the fact that around a third of merchants are still not reporting attacks.

Mexican merchants are the second most likely to report attacks at 78% but it's hard to ignore the 16% of merchants who aren't. As we've already mentioned, the region is dealing with a massive surge in fraudulent online accounts.

Merchants in the UK and Ireland are the least likely to report attacks at 43%. This is interesting as GDPR is very clear on a business's obligation when it comes to data breaches. Businesses must report personal data breaches to the ICO within 72 hours of becoming aware of the breach. This might just be a case of lack of awareness but it definitely needs to be addressed.

Almost 90% of Australian merchants said that they had reported account takeover attacks. Reporting here might be so high compared to some of the other regions thanks to a federal scheme for the mandatory reporting of cybersecurity breaches that result in the loss of personal data.

REPORTING OF ACCOUNT TAKEOVER ATTACKS **BY COUNTRY**



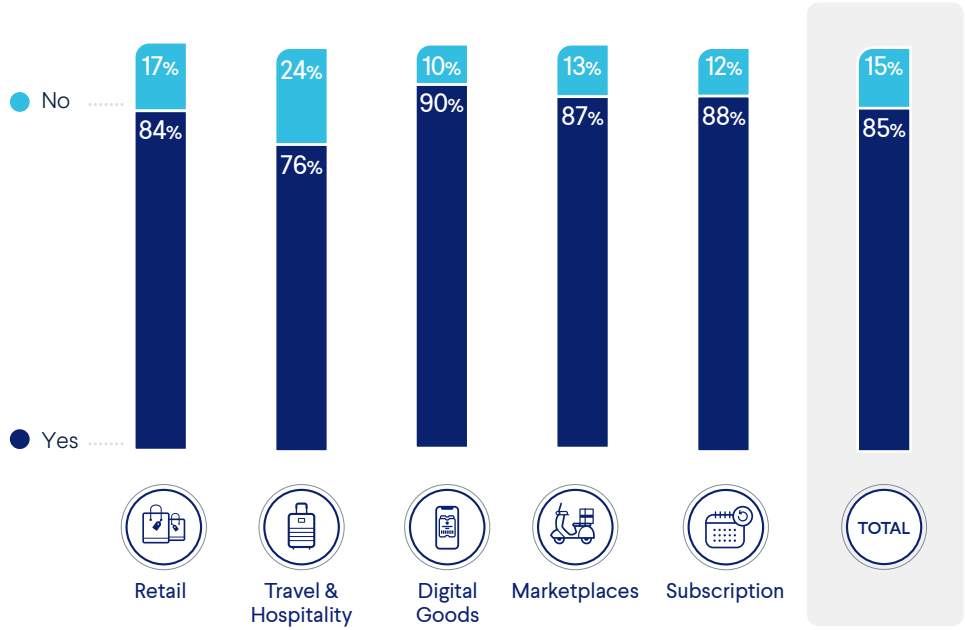
9.5 ACCOUNT RECOVERY PROCESS

Almost 90% of merchants across industries have some sort of process for recovering the accounts of account takeover victims.

A quarter of Travel & Hospitality merchants don't have a documented process in place, which is troubling because the industry has been experiencing increased account takeovers.

Why should you act fast on getting a process in place? Customer loyalty is vital to businesses, especially as both demand and competition are high. After an account breach, genuine customers don't want to have to start from scratch with a new account and lose all their loyalty points. Merchants need a straightforward account recovery process or they risk losing a loyal customer to a competitor.

INDUSTRIES WITH A DOCUMENTED PROCESS FOR
RECOVERING ACCOUNT TAKEOVER VICTIM ACCOUNTS

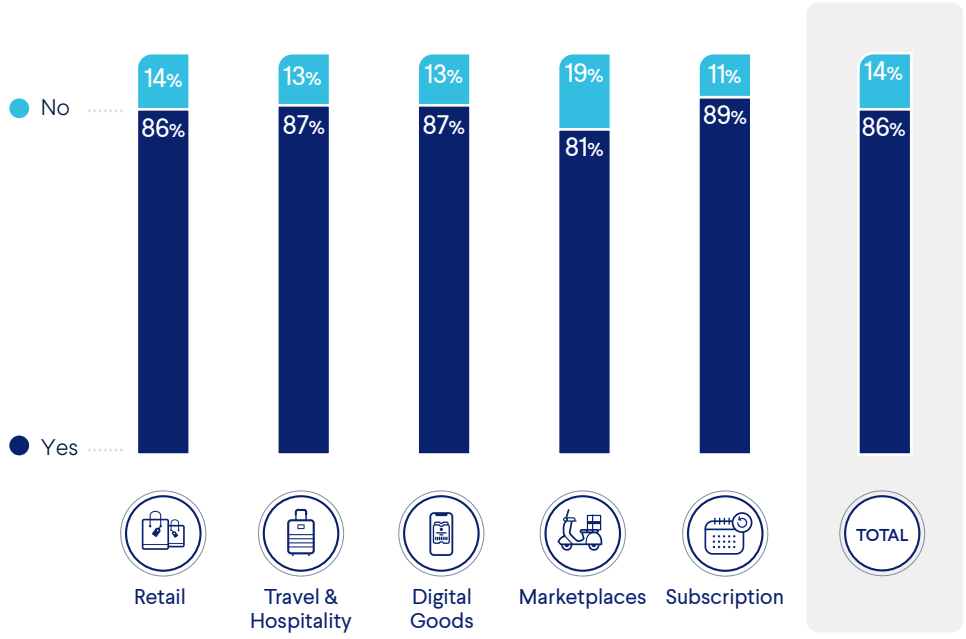


9.6 BREACHED CREDENTIALS DATABASE

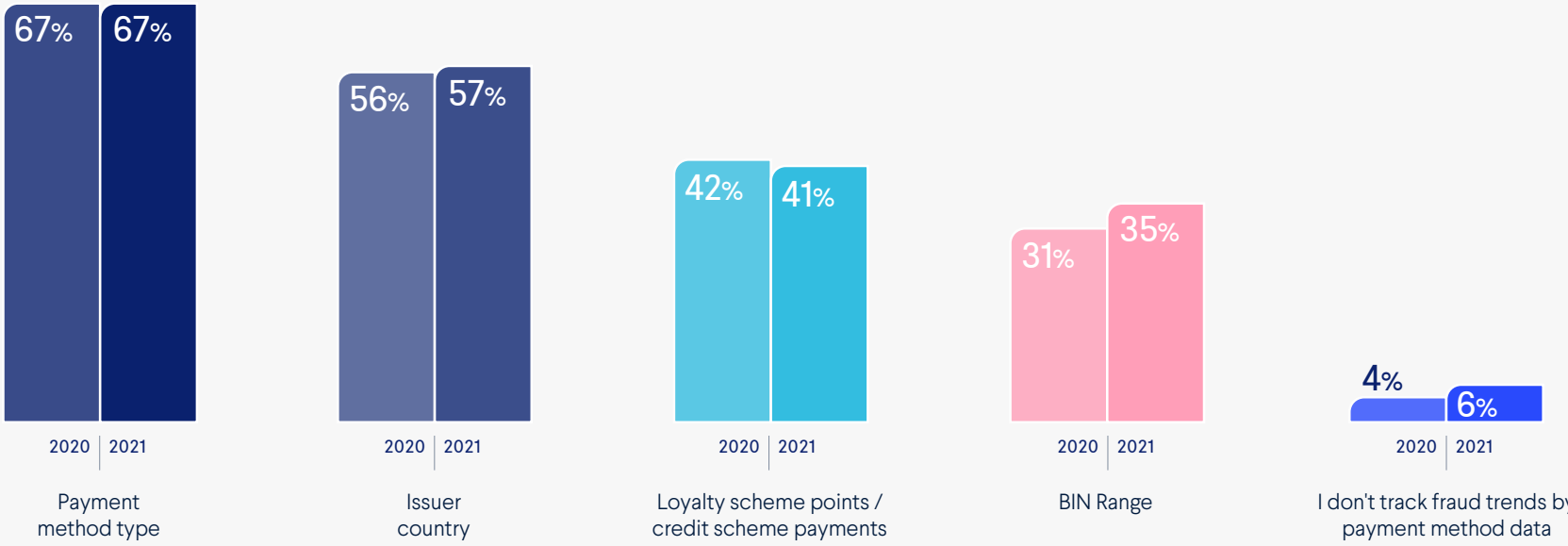
Over 80% of merchants across industries use a breached credential database. This is invaluable when it comes to fighting account takeover fraud.

In particular, **credential stuffing**. Maintaining a breached credential database offers protection against this by verifying whether credentials have been breached previously. **There are an estimated 8.4 million passwords currently circulating online**, more than 3.5 billion of which are tied to active email addresses.

BREACHED CREDENTIALS DATABASE



10.0
TRACKING FRAUD BY PAYMENT DATA



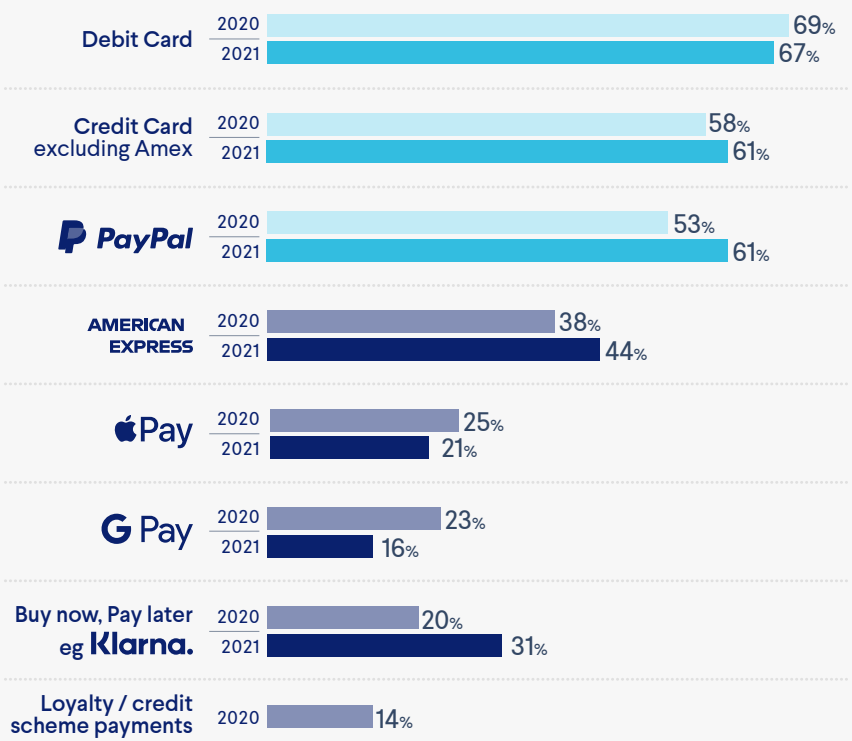
We asked merchants what types of payment data they are tracking. Payment method type is the most tracked piece of data at 67%. But for such valuable information, this is still quite low. Identifying the payment methods preferred by the fraudsters that target your business is vital for fraud prevention.

Only around a third of merchants track BIN ranges. And it is still the least tracked piece of payment data. This is despite a **significant surge in BIN attacks** and card-related fraud losses since the start of the pandemic. Yes, **issuers and PSPs are usually the targets of BIN attacks.** But this still exposes merchants to larger-scale fraud attacks.

Tracking payment data will inform your fraud prevention strategy and allow you to quickly identify potentially risky transactions. This is particularly important when it comes to optimizing exemptions from strong customer authentication SCA, which we will discuss later.

10.1 TOP 3 PAYMENT METHODS FOR FRAUD

We asked participants for the top three payment methods that they saw the most fraud in.



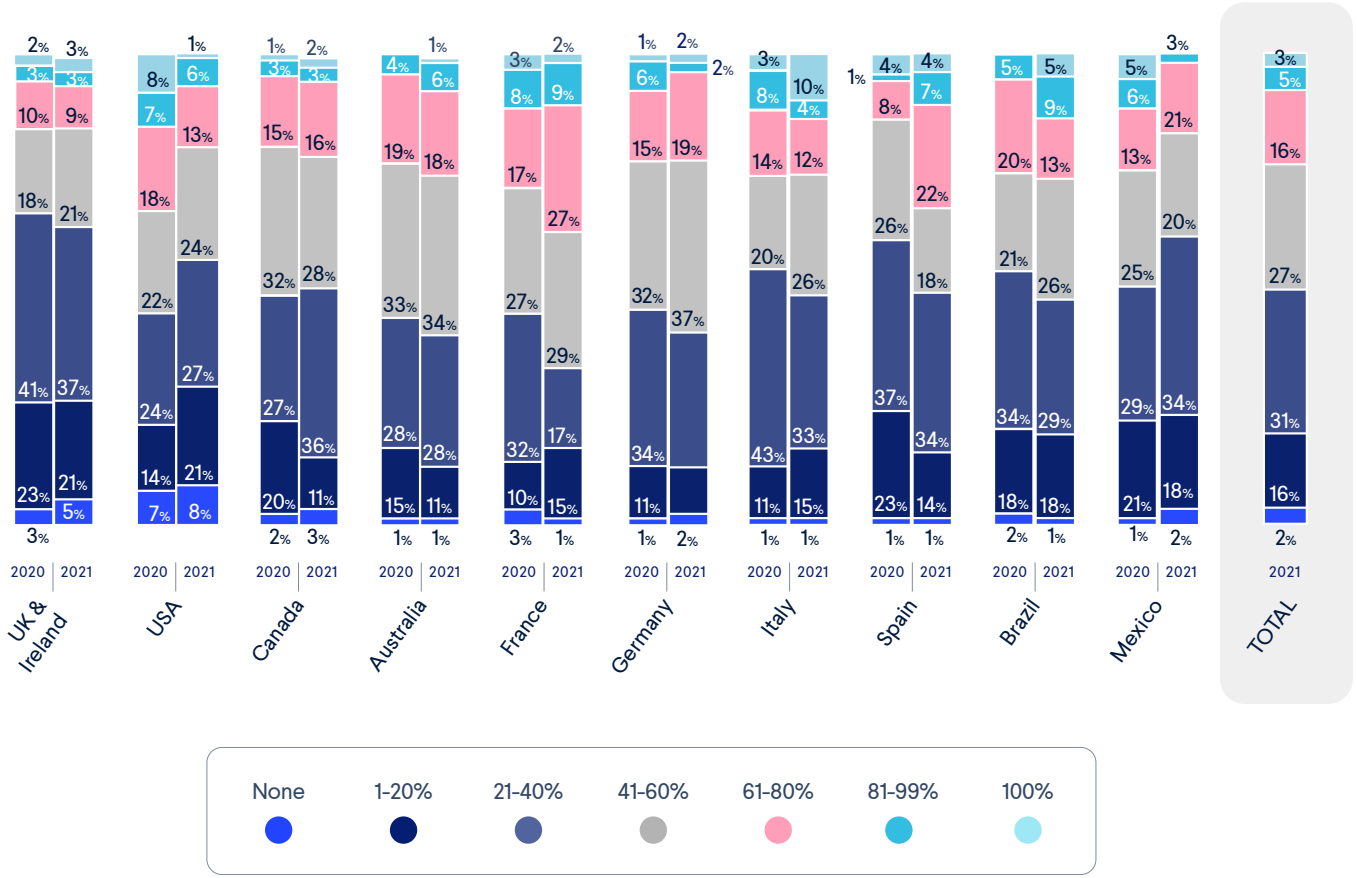
Debit cards and non-American express credit cards are the most fraudy for merchants. But this isn't too surprising. Traditional bank cards are the most commonly used payment method in many markets, and fraudsters like to hide in plain sight.

Over 60% of merchants consider PayPal to be a top method for fraud. PayPal seems to be shooting up the ranks as a primary avenue for fraudsters. In fact, **PayPal credentials are now worth more** on the dark web than credit card credentials.

Interestingly, the combined percentage of merchants that consider Google Pay and Apple Pay to be fraudy payment methods is much lower than for PayPal. This could be because these digital wallets allow users to take **advantage of security features** on their mobile device such as biometric authentication. So they are often considered to be low-fraud. However, our research has found that cards are often not fully authenticated when added to a wallet, making them a top vehicle for fraudsters using stolen credit card details. This is a growing issue that you should be aware of.

10.2
3D SECURE TRANSACTIONS BY COUNTRY

TRAFFIC SENT TO 3DS
BY COUNTRY



Almost 10% of US merchants sent no transactions through 3DS in 2021, which is rather high. SCA is not currently mandated in the USA, but merchants would be well advised to consider this extra layer of security to tackle rising fraud. As SCA mandates expand beyond Europe, fraudsters will likely turn their attention to countries with lower barriers to entry. We're already seeing fraud of all types rise at a faster rate than those in the UK or Europe.

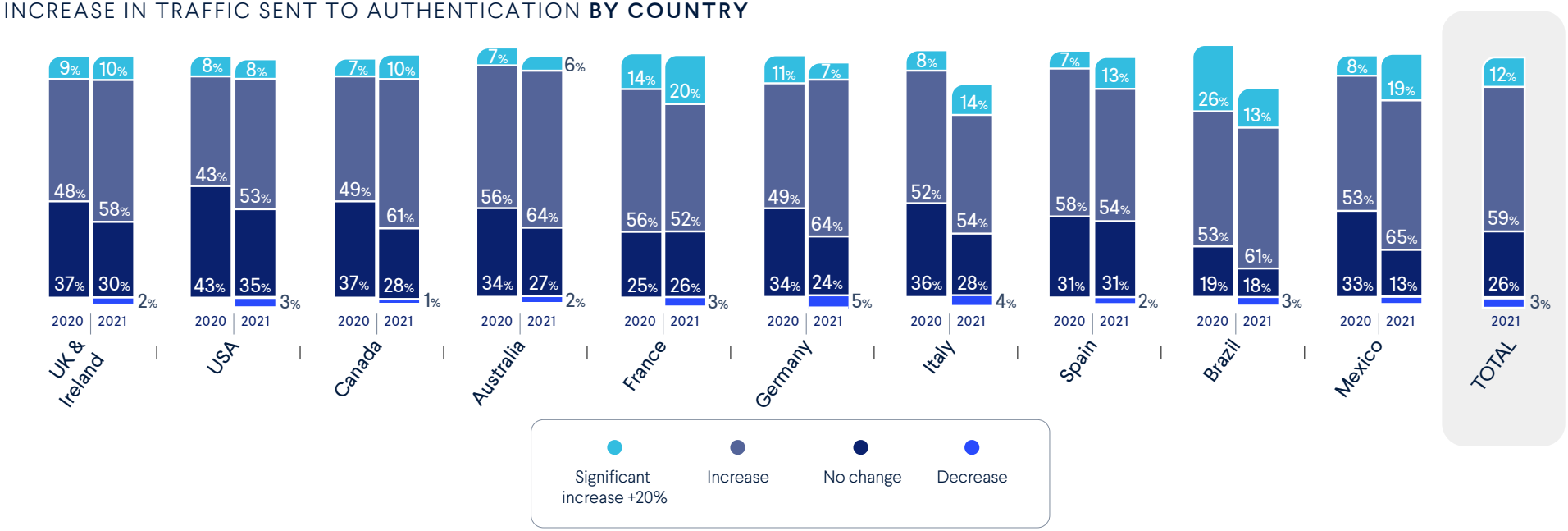
SCA will fully come into force in the UK by 14 March 2022 and merchants must adhere to the new rules or risk customer purchases being declined. So it's interesting that the percentage of UK and Irish merchants that are sending over 40% of their transactions through 3DS has only marginally increased. As the mandate comes into full effect, we are likely to see traffic sent through 3DS increase, but savvy merchants will be looking for ways to exempt their transactions where possible.

10.3 INCREASE IN TRAFFIC SENT TO AUTHENTICATION BY COUNTRY

Over 70% of merchants across regions report sending more transactions for authentication over the past year. We've seen increasing **secure and adaptive payment authentication methods** become a key business strategy for many companies globally.

As the ecommerce market continues to grow, taking the best practices of SCA and using new authentication approaches will be hugely beneficial for merchants, regardless of country. It will allow multinational businesses to offer a more consistent experience while ensuring both ease of use and security. It's only a matter of time before regulations requiring adherence to similar standards begin to spread outside the UK and Europe. How are you preparing for SCA, if at all?

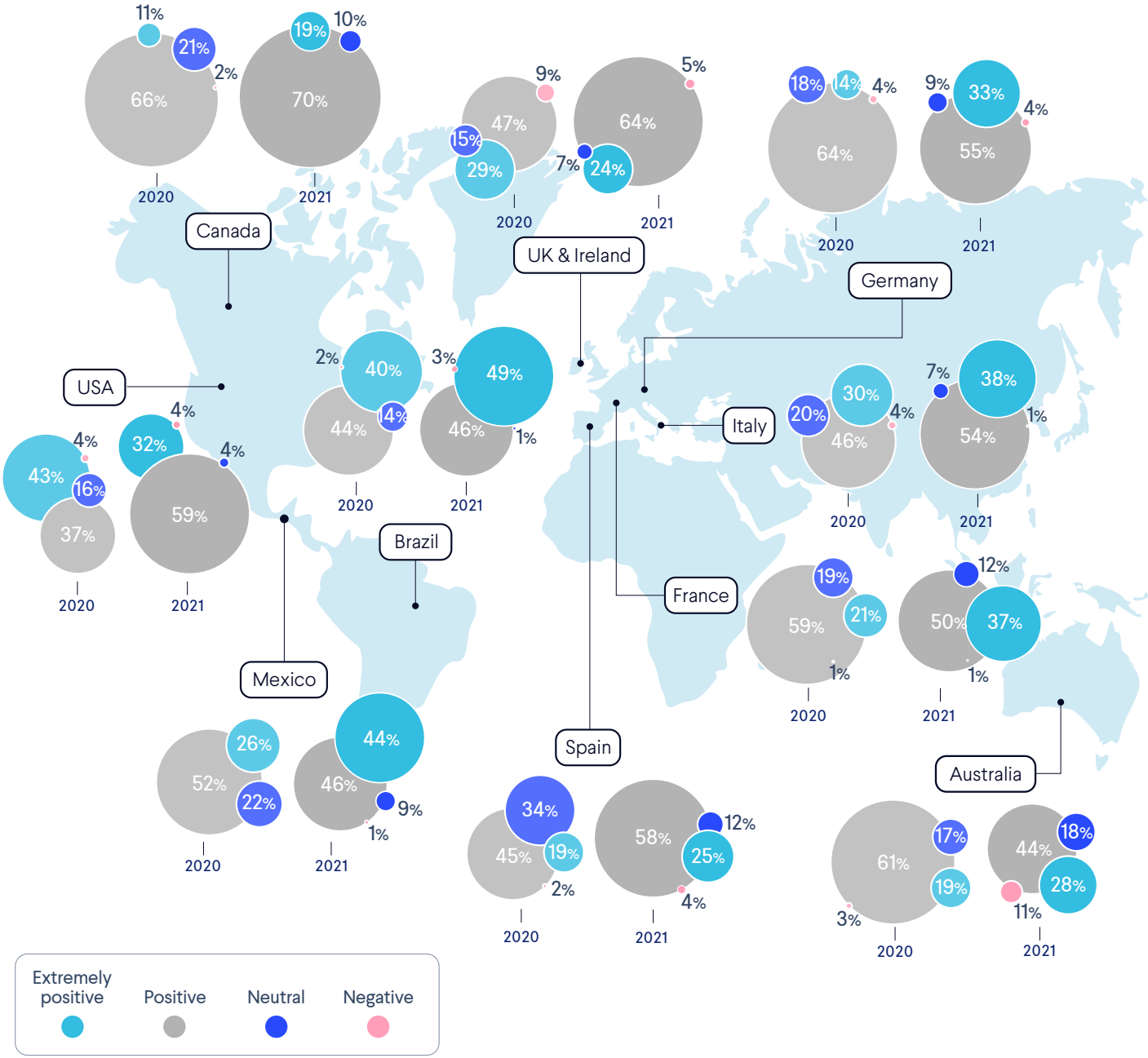
INCREASE IN TRAFFIC SENT TO AUTHENTICATION **BY COUNTRY**



11.0 PSD2 PERCEPTION BY COUNTRY

We wanted to get a temperature check and see how merchants globally are feeling about PSD2. And almost 90% of the merchants who are aware of PSD2's impact believe it will be positive.

PSD2 was introduced in the hopes of **stimulating growth and competitiveness** in the EU financial sector and addressing the rapid growth of ecommerce fraud. To combat fraud, it introduces new standards for multi-factor authentication. The latest version of 3D Secure is seen by some as **proof that strong security and great customer experience (CX) can co-exist.** This could be why we are seeing an increasingly positive outlook – SCA as part of PSD2 will allow you to better balance security and conversion.



11.1 USE OF EXEMPTIONS BY INDUSTRY

After a rough first pass, the SCA mandate now comes with some exceptions that aim to support a **frictionless customer experience when transaction risk is low.** There have always been concerns around the added steps required by SCA, which can lead to abandoned carts at checkout. In 2014 this change in India cost some businesses around a **quarter of their sales**.

40%

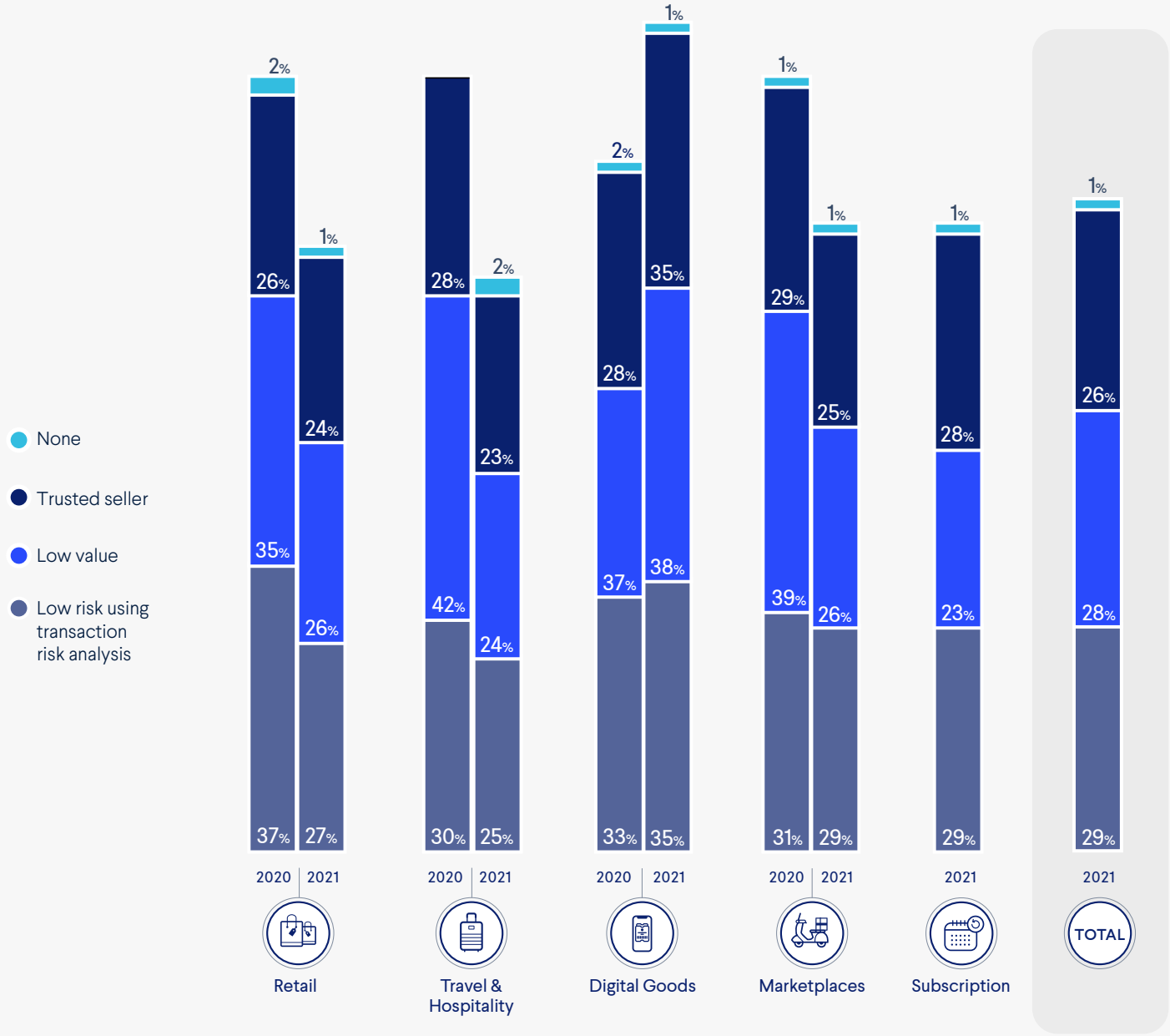
Digital Goods merchants intend to use low value payment exemption

Exemptions mean that your trusted customers with low fraud rates don't have to go through additional authentication, allowing merchants to strike a balance between managing risk and optimizing conversion. So it is surprising to see that only around a quarter of merchants plan to use each of the exemptions available as part of their PSD2 strategy.

Of all industries, Digital Goods merchants are the most likely to use each of the exemptions. Almost 40% intend to use the low value payment exemption. This would allow them to avoid applying SCA on payments **under €30 up to a certain cumulative limit.** This could be because Digital Goods merchants are more likely to sell individual products of a lower value. For example, in-app gaming purchases are unlikely to exceed the limit.

It is vital that you are analyzing and segmenting your transactions to understand the potential for exemptions. But remember - 3DS is not free! There is a cost to each authentication and this will quickly add up. Working with your issuer to make the most of the exemptions available to you could save your business money.

USE OF EXEMPTIONS **BY INDUSTRY**

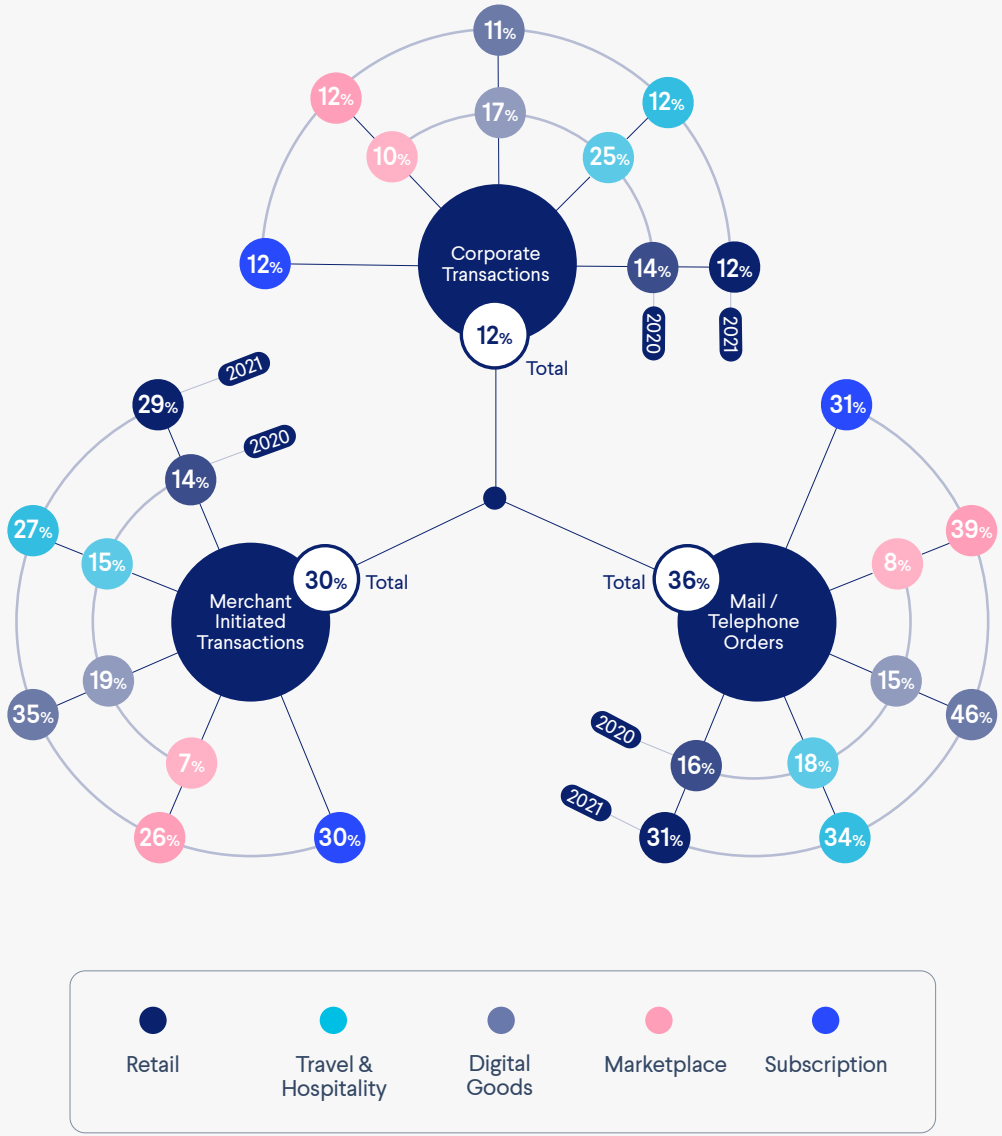


11.2 TRANSACTIONS OUTSIDE THE SCOPE OF PSD2 INCREASE BY INDUSTRY

Not all transactions are covered by PSD2, so whether or not you apply SCA on them is up to you. Of the areas that aren't covered by PSD2, around 40% of merchants believe that mail and telephone orders will see an increase in fraud.

Almost 50% of Digital Goods merchants feel this way. This is a worry because, as we've already touched upon, the number of merchants tracking fraud by call center has dropped since 2020 across the board. Since the start of the pandemic, we have seen an increase in **fraudsters targeting customer services** using social engineering techniques. Even **Apple has fallen victim!** PSD2 is here to help but don't let it lull you into a false sense of security.

TRANSACTIONS OUTSIDE THE SCOPE OF PSD2 INCREASE **BY INDUSTRY**



12.0 SUMMARY

This survey provides valuable, in-depth understanding into merchant fraud teams, their environment and forecasts. The high-level insights also highlight where further investigation and discussions can enable merchants to boost their fraud detection ability and gain deeper knowledge on their customers and the threats they face.

1 COVID-19 IMPACT ON BUSINESS HAS BEEN POSITIVE, AS ORDER VOLUMES SKYROCKET

The majority of merchants have seen the business impact of the Covid-19 outbreak improve over the year. Digital Goods and Subscription businesses have the most positive outlooks, whereas Travel & Hospitality is still experiencing more adverse effects from the pandemic. All merchants have seen order volumes increase, but profits haven't necessarily followed.

Fraud levels remain high, but new fraud types are emerging. Hardly any merchants are seeing less fraud than pre-pandemic. Merchants are more focused on stopping fraud and fraud teams are getting more appreciation.

2 FRAUD TEAM DYNAMICS CONTINUE TO IMPROVE

As forecast in 2020, the majority of fraud teams have grown over the past year, and will continue to grow in 2022. Predicted growth over the next year is slightly less dramatic, but it's clear that expanding online operations is at the center of business leaders' strategies going forward, as CFOs and CROs are the driving forces behind increasing fraud prevention investment. Fraud team perception has improved in-step. Budgets will still increase, but more tentatively than in 2021.

3 INNOVATION IN TOOLS & INCREASING BUDGETS CONTINUE TO RAMP UP

The number of merchants using in-house tools only has dropped, and those that outsource the majority of tools has risen. But overall a mix is still preferred. Rules are still considered an important part of the fraud toolbox. Machine learning and text verification are becoming increasingly popular.

4 ONLINE PAYMENT FRAUD AND ACCOUNT TAKEOVER ARE TOP THREATS, BUT POLICY ABUSE IS GROWING FAST

Fraud has grown in 2021 even more than it did in 2020. Online payment fraud has increased significantly and account takeovers have increased for over half of merchants, but refund abuse has grown the most. Merchants are starting to switch on to the risks of promo and refund abuse. LatAm fraud, particularly in Mexico, is rising faster than in any other country.

5 INDICATORS OF FRAUD VARY BY INDUSTRY GROUP AND INDIVIDUAL BUSINESS TYPE

Account history and order costs are most important to merchants overall, but it depends on every individual merchant's fraud signals. Tracking orders on the web, apps and via discounts has increased, as merchants settle into the digital shift. Fraud teams tend to spend from 20-60% of their time on manual review, and an increasing amount of time on dispute management.

6 FEW MERCHANTS ARE LOOKING AT PAYMENT DATA TO DETERMINE FRAUD

Over a third of merchants are still not tracking payment data to help inform risk decisions. PayPal is considered the most risky payment method, after debit and credit cards. There's not been much change in how many transactions merchants are sending through 3DS over the year.

7 GLOBAL CONFUSION ABOUT THE IMPACT OF PSD2 REMAINS

The majority of merchants wrongly believe that 3DS will remove the need for fraud tools. There's still confusion globally on the impact of PSD2, with over 50% thinking it won't impact business. Globally, almost all merchants who are aware of PSD2 think it's impact will be positive, and many are keen to utilize 3DS exemptions to reduce checkout friction.

Thank you for reading our fraud and payments survey report

If you have any questions, feedback or comments please get in touch via the website.

GET IN TOUCH

Learn more about Ravelin's fraud and payments services at

ravelin.com