Ravelin

# ONLINE MERCHANT PERSPECTIVES

## FRAUD & PAYMENTS SURVEY 2020

ravelin.com

# CONTENTS

# 1.0 INTRODUCTION

2020 has been a challenging year for online merchants. Regulations such as Europe's Second Payment Services Directive (PSD2) are gaining momentum, forcing businesses to rethink conversion strategies. Globally, the Covid-19 outbreak led to a huge surge in online transactions, with this shift in priorities bringing its own challenges.

As well as changes in the macro environment, fraudsters are always evolving their methods. Many merchants have seen growth in new forms of fraud activity including account takeover, promotion and refund abuse. How well-equipped are merchants to deal with the threats they face? Our findings suggest there are some holes in their armor which merchants must address to ensure their businesses are protected.

**This report provides insights into:**

- Merchant perceptions of how fraud is changing and top business threats
- Tools, budgets and methods for monitoring fraud and false positives
- The macro environment impact, including Covid-19 and PSD2

**Survey methodology**

This quantitative survey was commissioned by Ravelin and carried out by Qualtrics using a panel of 1000 fraud professionals from countries around the world in August 2020. Survey participants work for online merchant businesses with over $50million in annual revenue. The survey was translated into each respondent's local market language for clarity.

# 2.0 SURVEY SAMPLE CHARACTERISTICS

## INDUSTRY, LOCATION AND JOB ROLES

Our survey participants are fraud and payments professionals from around the globe. These professionals work in key ecommerce markets in Europe, Australia, North and South America.

**Survey participants work in a range of business industries under four main groups:**

**Retail**
Including health and beauty, groceries, fashion, electronics and fast moving consumer goods (FMCG).

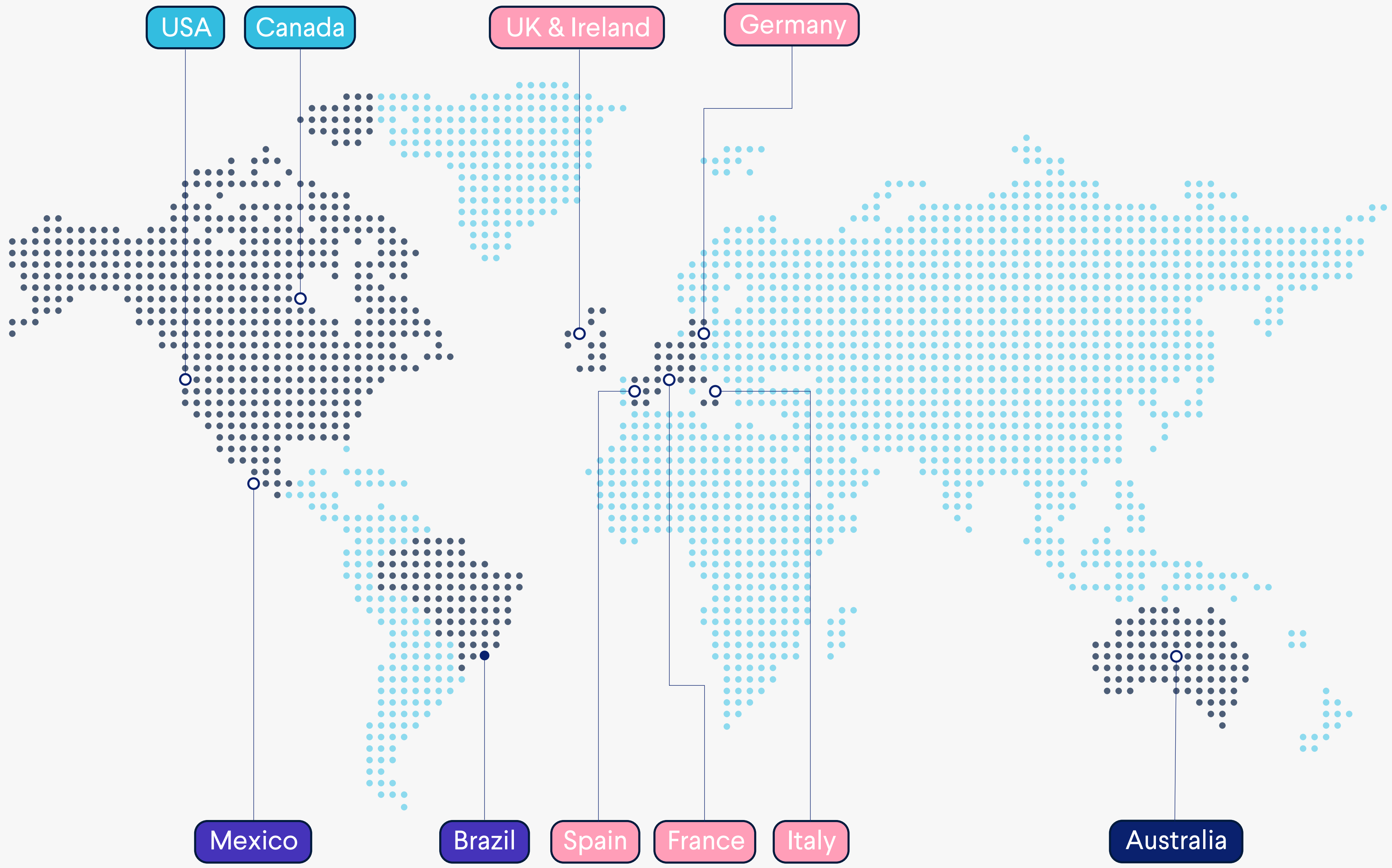
**Marketplaces**
Including taxi/cab service providers, food delivery and other product/service delivery businesses.

**Travel and hospitality**
Including accommodation booking and transport /travel ticketing.

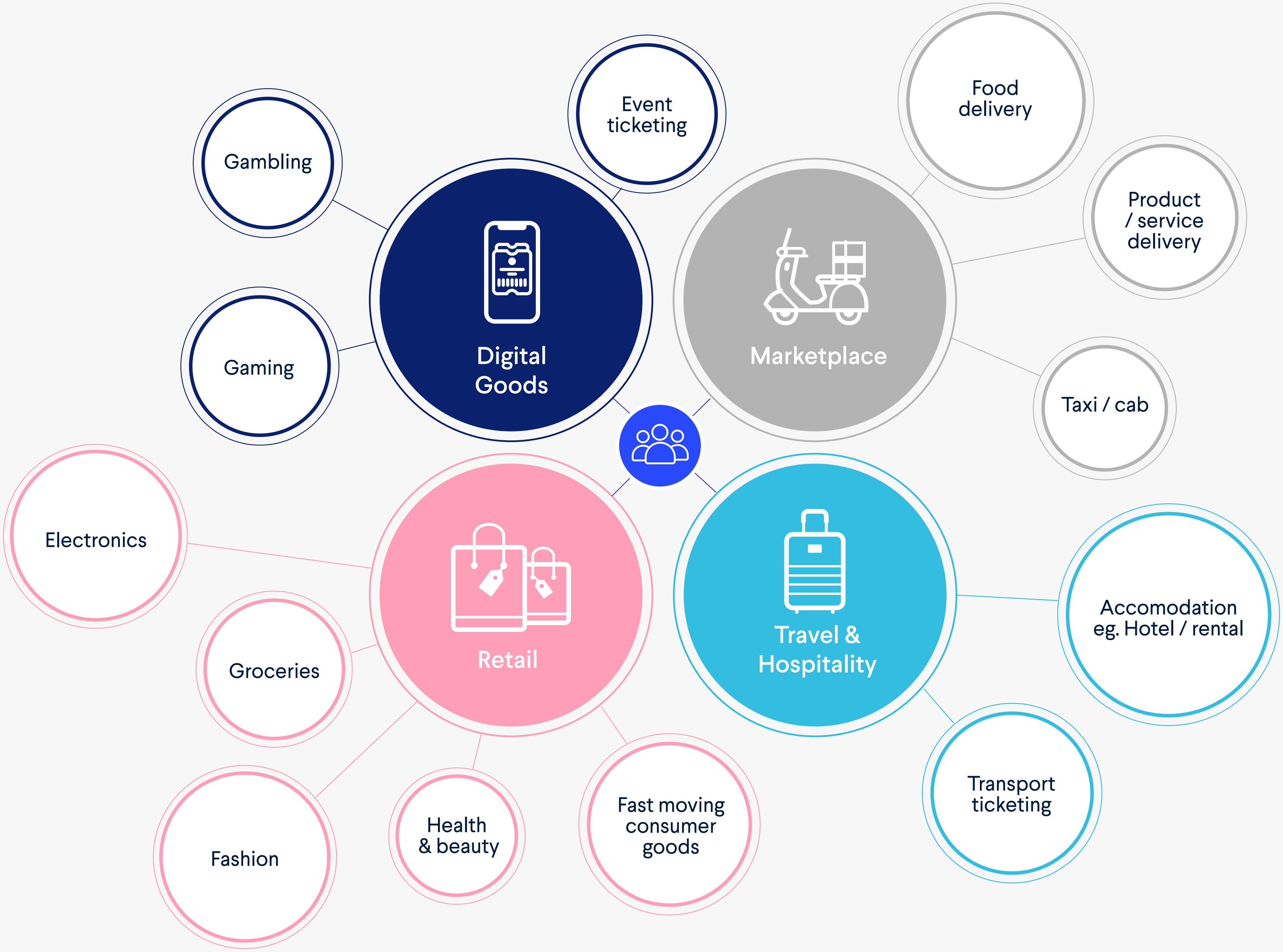
**Digital goods**
Including gaming, gambling and event ticketing.

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 over 40% at C-Level.

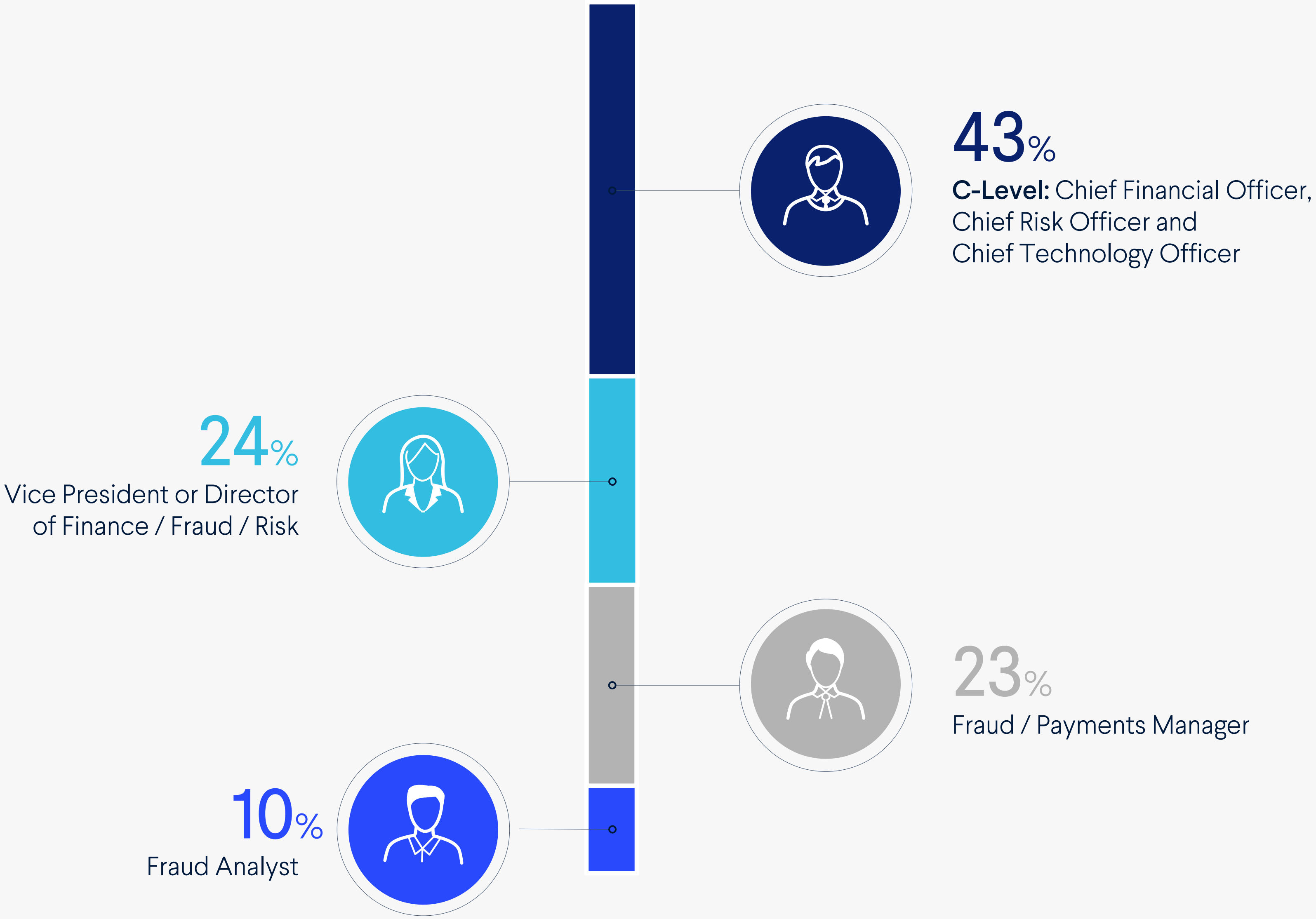
## SURVEY PARTICIPANT COUNTRIES



## SURVEY PARTICIPANT INDUSTRIES



## SURVEY PARTICIPANT **JOB ROLES**



43%
**C-Level:** Chief Financial Officer, Chief Risk Officer and Chief Technology Officer

24%
Vice President or Director of Finance / Fraud / Risk

23%
Fraud / Payments Manager

10%
Fraud Analyst

# 3.0 THE COVID-19 EFFECT

## Global pandemic impact on fraud teams

**46%**

**of all participants said that the global Covid-19 pandemic impact on their business fraud operations was either positive or very positive.**

In April 2020, approximately **one-third of the world's population** had been placed on some form of coronavirus lockdown. This in turn caused a rise in ecommerce transactions globally. For example **in the UK,** online retail order volumes rose by over 200% on some products. The rise in ecommerce transactions peaked during the height of restrictions, but there is still a significant increase in **online shopping activity** compared to pre-pandemic levels.

Likewise, delivery services became in high demand due to social-distancing measures, with a **surge in food delivery** driven by consumers being unable to dine in restaurants and many restaurants offering takeaway options.

This huge rise in online transactions could explain why at the time of this survey, more merchants see Covid-19 as positive than negative.

46% of all participants said that the global Covid-19 pandemic impact on their business fraud operations was either positive or very positive. Positive here could be in the sense that they are busier with more volume. We could also assume that fraud operations have become more important to a business strategy, as the shift in focus turns to ecommerce.

## Is a massive rise in transactions always good for the fraud team?

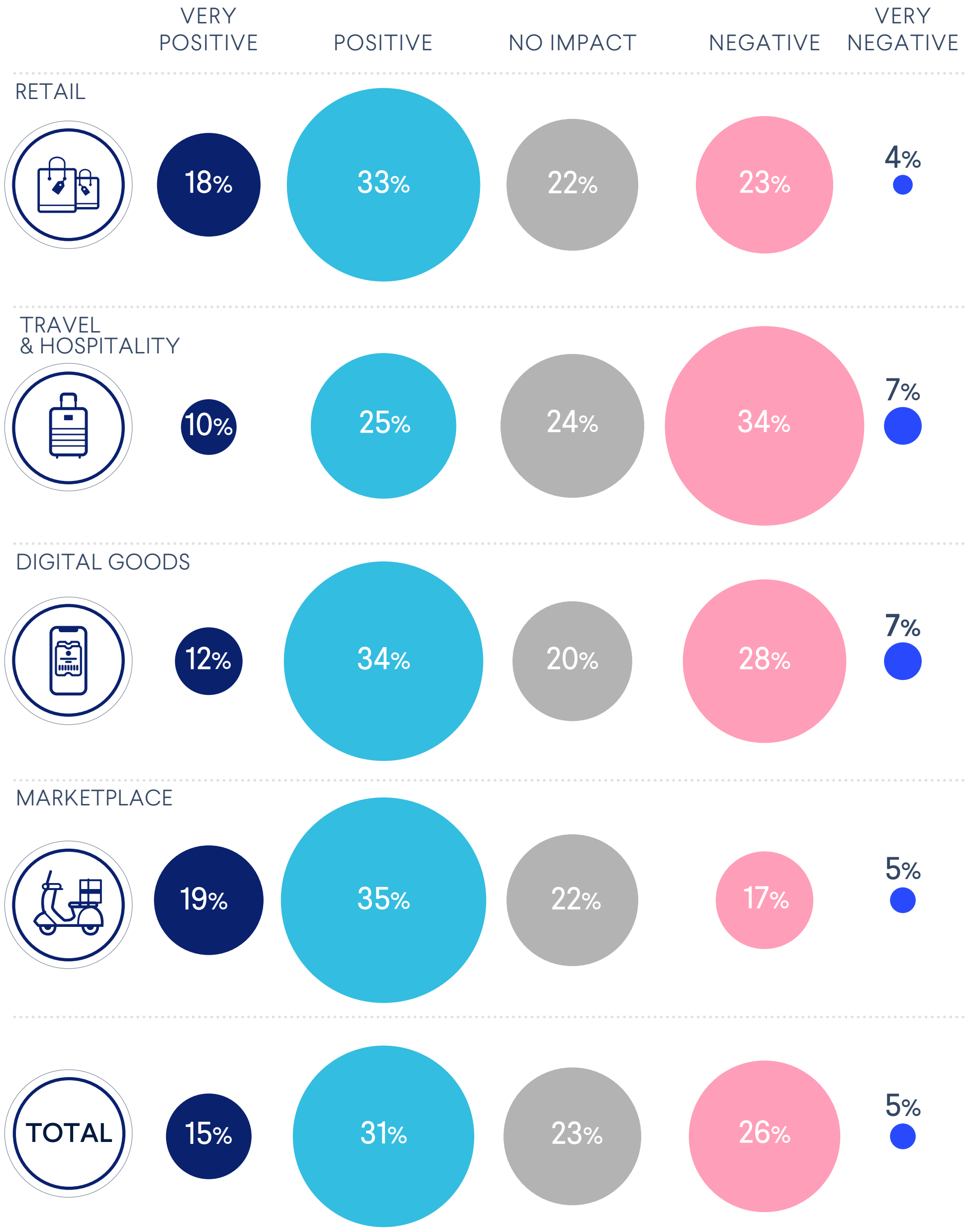
In some ways, this can make the fraud teams role more challenging, particularly if there are new accounts with no purchase history. However, we have seen that Covid-19 has forced merchants to take a different approach to orders. A number of businesses restricted orders to existing customers and blocked new account registrations - for example in the UK, **even the online-only supermarket Ocado struggled with the demand surge**. This often meant that even though transaction volumes increased, the overall percentage of fraud went down.

The Travel & Hospitality sector viewed the impact as the most negative, with 41% saying it had a negative/very negative impact on their fraud operations. This makes sense, as this sector has been hardest hit by the Covid-19 pandemic restrictions on movement.

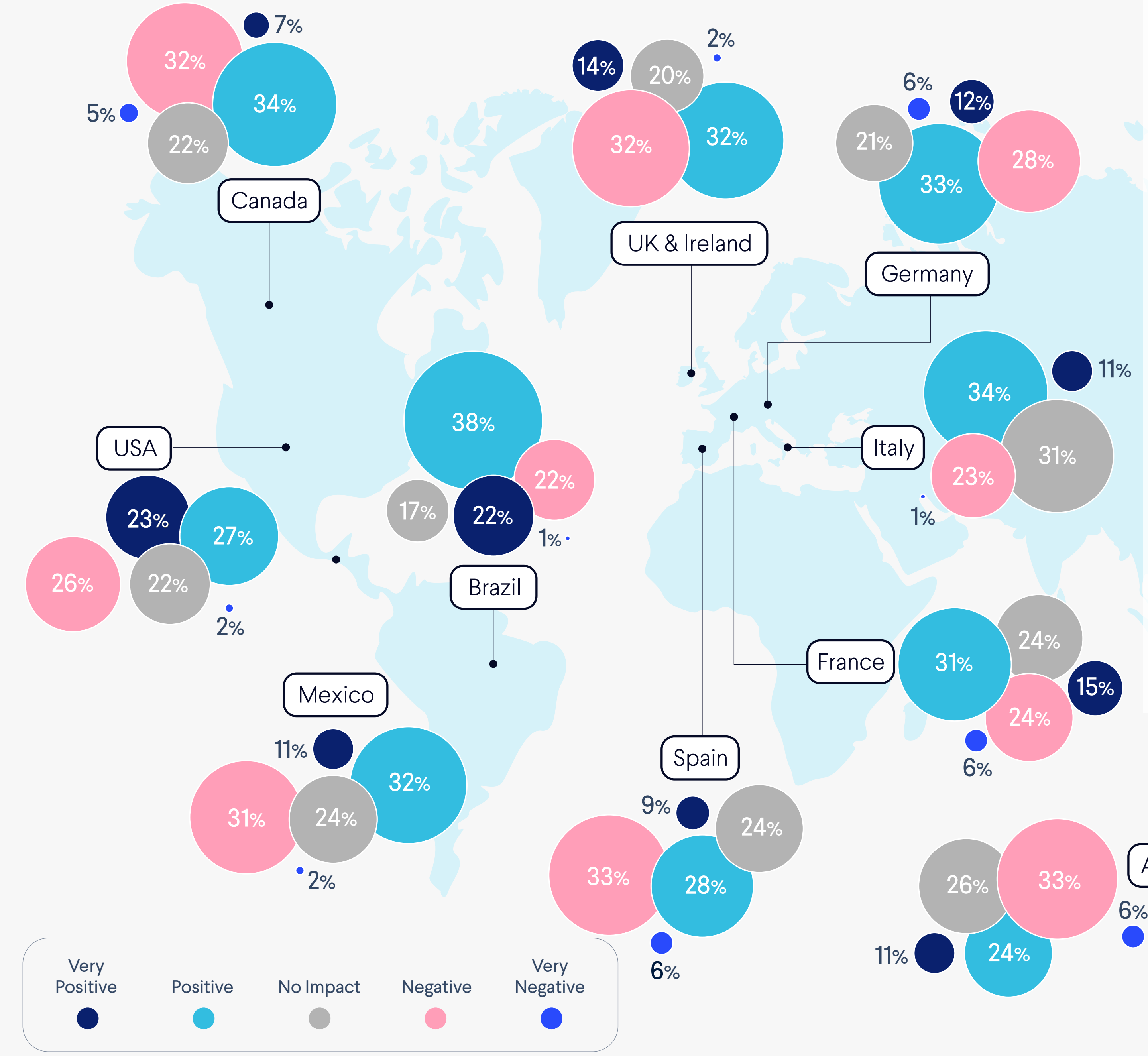
41%

**Travel &Hospitality merchants said Covid-19 has had a negative impact on their business fraud operations**

## IMPACT OF COVID-19 **ON INDUSTRIES**



## IMPACT OF COVID-19 **ON FRAUD TEAMS GLOBALLY**



**Globally, there's not a wide difference between the perceived impact of Covid-19 on fraud teams. However, it's notable that fraud teams in two typically fraudy locations perceived the impact as very positive: the USA and Brazil.**

Why might this be?

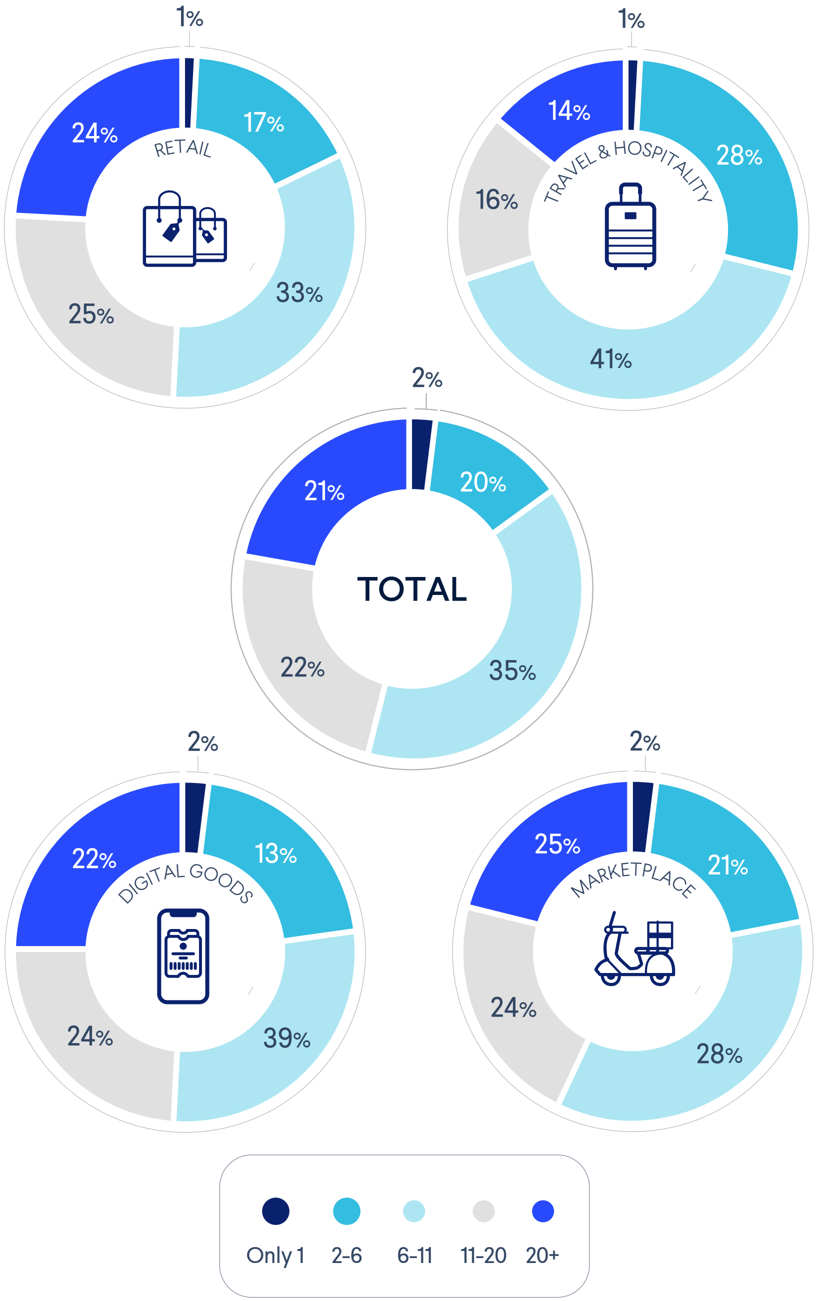
In Brazil, the Covid-19 pandemic overlapped with a reduction in the ratio of fraud to online transactions. **Mercado & Consumo reported** that online sales grew faster than online fraud attempts between January and May 2020, with attempted fraud accounting for 1.5% of transactions, compared to 3.47% in 2019. However, this might change as the surge in online shopping stabilises and fraudsters adapt to the new climate.

# 4.0 FRAUD TEAMS

## Size and growth predictions

Overall, 60% of fraud teams have between two and ten people, with over one-third between six and ten. Retail, Digital Goods and Marketplace teams are likely to be larger, with 48%, 46% and 49% of participants having 11 or more team members respectively.

NUMBER OF PEOPLE IN THE **FRAUD TEAM**

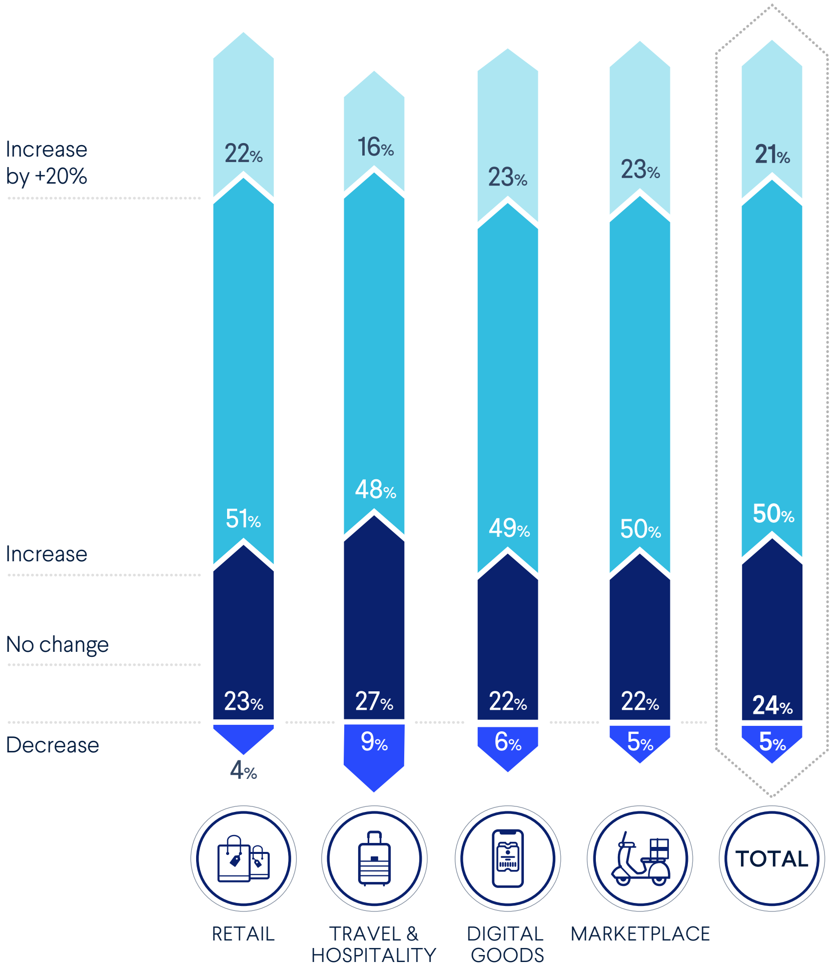


Over 70% of businesses expect their fraud team to increase in the next year, with none predicting a significant team reduction. This reflects a trend across all industry sectors to invest in online operations, with fraud management an important part of this. This is reassuring for fraud professionals, as even in the worst-hit Travel & Hospitality sector, the overall trend of increasing team size is counter to the **global prevailing bad news on jobs** and employment.

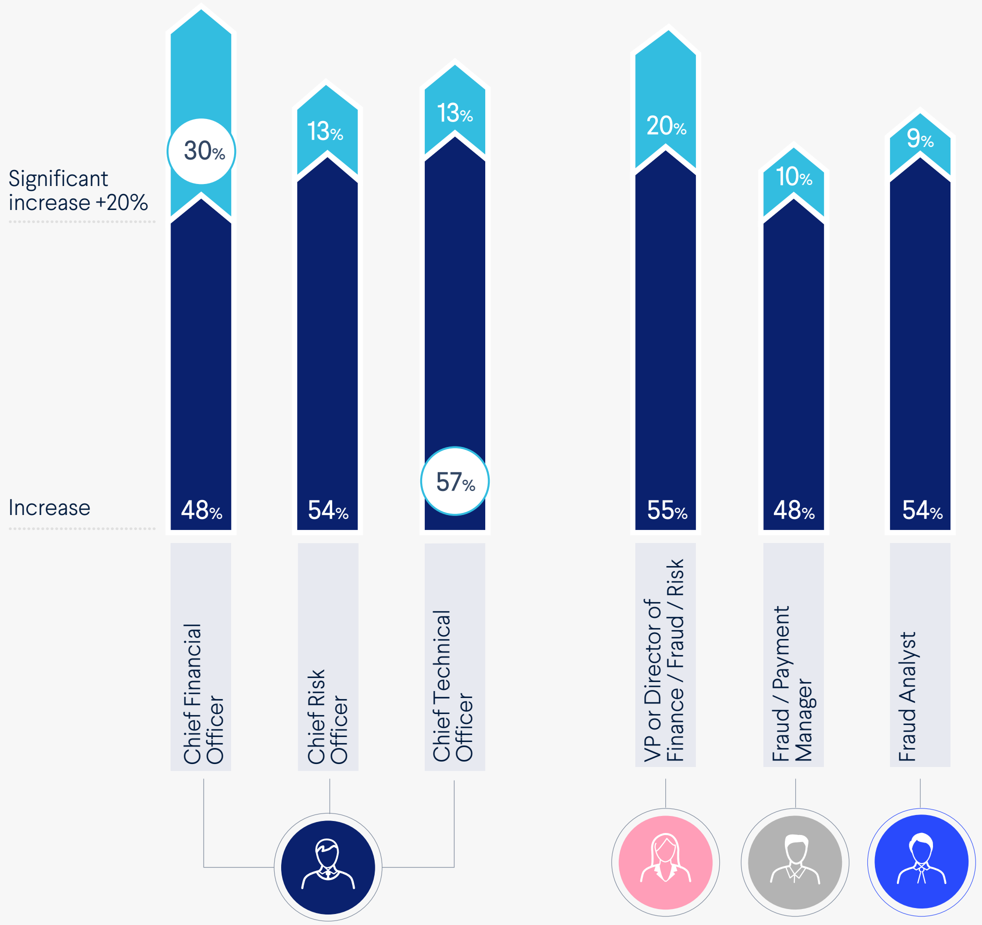
**OVER 70%**

**of merchants expect their fraud team to increase in the next year**

## PREDICTIONS OF FRAUD TEAM GROWTH BY INDUSTRY



## PREDICTIONS OF FRAUD TEAM GROWTH BY JOB ROLE



ALMOST **80%** of CFOs predicted an increase in the fraud team

Almost 10% of fraud professionals in Travel & Hospitality predict a team reduction in the next 12 months. This figure is still very low when considering the more negative impact of Covid-19 on the industry, highlighting the continued importance of having a fraud team to secure whatever business continues online. It's important to note that the survey was carried out in August 2020, and the Covid-19 impact on the travel sector is likely to change as countries adapt their restrictions on movement.

Interestingly, CFOs are most likely to predict a significant increase in the fraud team, with almost 80% predicting an increase, of which 30% predict significant team growth. Again, this is a reassuring sign for fraud professionals - however it may suggest that the positive outlook for the fraud team job security has not been passed down the business effectively.

# 4.1 FRAUD TEAMS

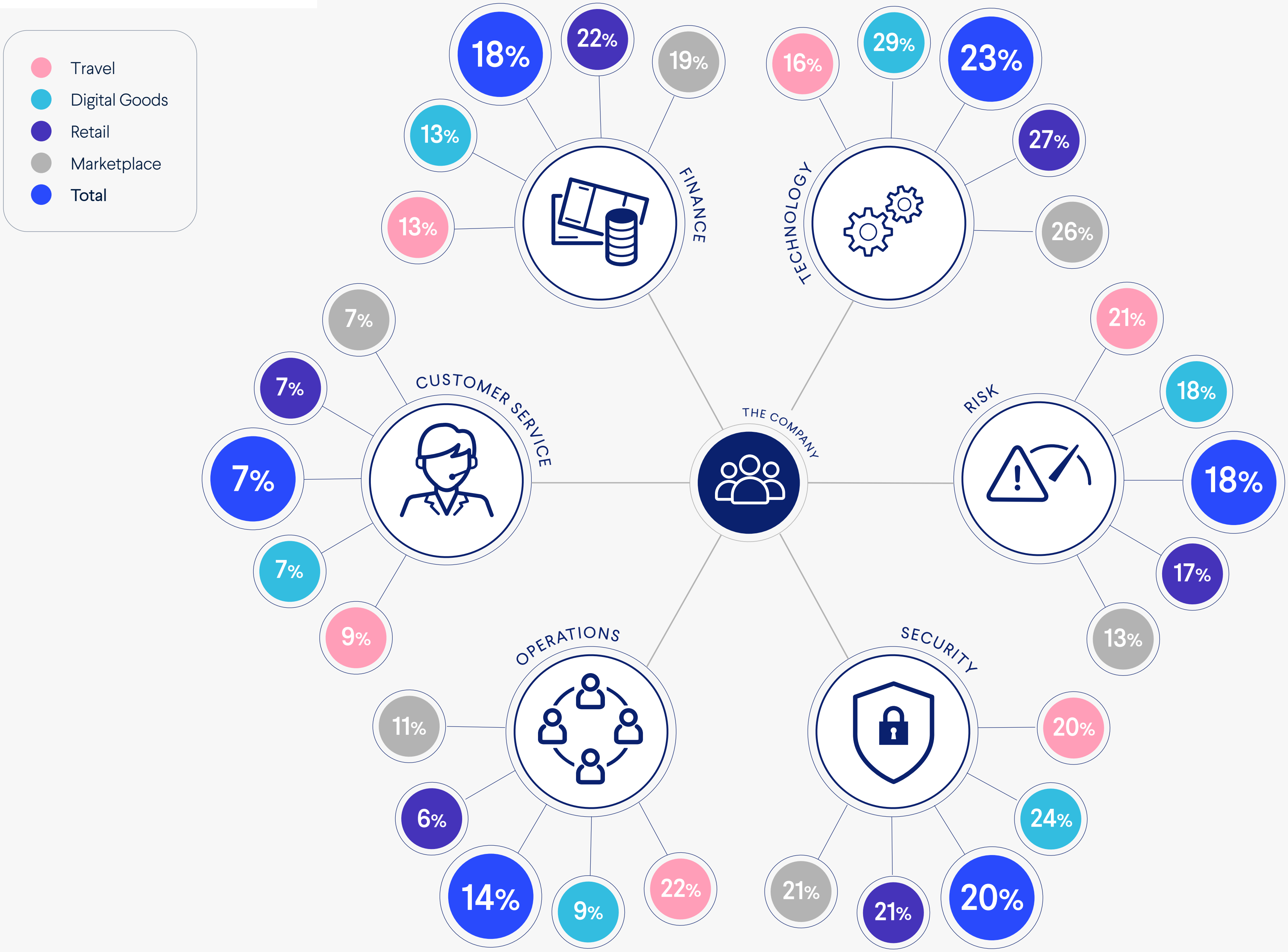
## Business department

Traditionally, fraud has been viewed as part of the business finance operations, but now the most common home for the fraud team is in the Technology department. Almost a quarter of all fraud teams sit in their business Technology department, this is higher for Retail, Digital Goods and Marketplace businesses.

Although Technology is the most common department, it still only accounts for 23% overall. Clearly, one size doesn't fit all, and there is not a stand-out majority in terms of which department the fraud team sits in. This reflects the broad nature of fraud, involving financial forecasts, account security, customer payment details and fraud tradecraft investigations.

Relatively few fraud teams are in the Customer Services department, but this is more likely in Marketplace and Travel & Hospitality sectors, perhaps reflecting the immediate sales environment, and the importance of speaking with customers directly.

# FRAUD TEAM DEPARTMENT **WITHIN THE BUSINESS**

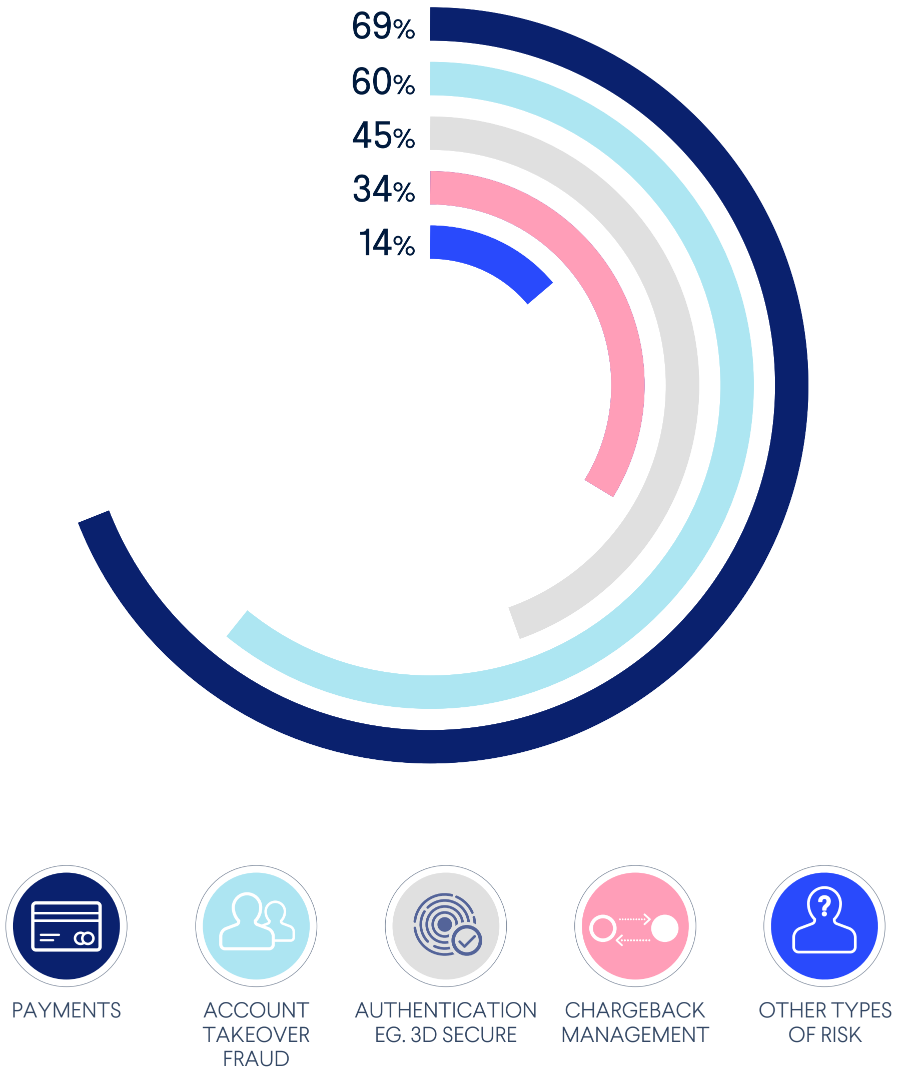


# 4.2 FRAUD TEAMS

## Team responsibilities and recruiting priorities

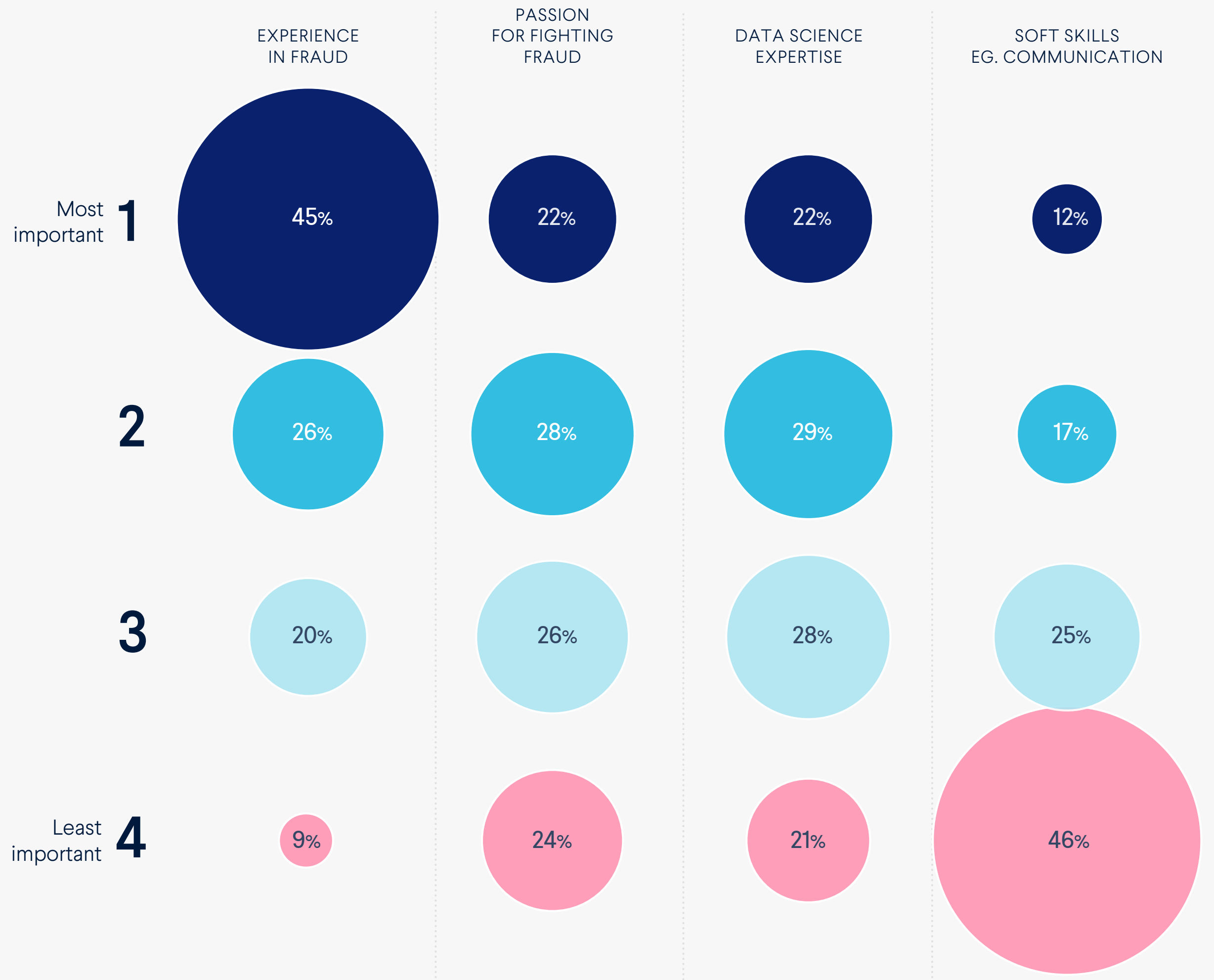
The cross-department nature of the fraud team is also reflected in the range of responsibilities. Almost 70% of respondents said their team is also managing payments for the business, however only 45% are also managing authentication. 60% of fraud teams are managing ATO fraud. This suggests that, similar to CNP fraud, it's challenging for businesses to decide who should have ownership of ATO and where it fits in the business structure.

RESPONSIBILITIES OF THE **FRAUD TEAM**



Experience in fraud was the most important requirement when recruiting into the fraud team. It may surprise some that data science expertise was the top requirement for only one quarter of participants, tied with a candidate's passion for fighting fraud.

## RECRUITING PRIORITIES



# No.1

**Experience in fraud was the most important requirement when recruiting into the fraud team.**

# 4.3 FRAUD TEAMS

## Perception within the business

Almost three-quarters of participants report an improvement in the wider business perception of the fraud team in the past year. This strongly correlates with the impact of Covid-19 on the business, and supports the idea that as businesses are more reliant on their online operations, fraud teams are being viewed as a more integral and critical function.

ALMOST

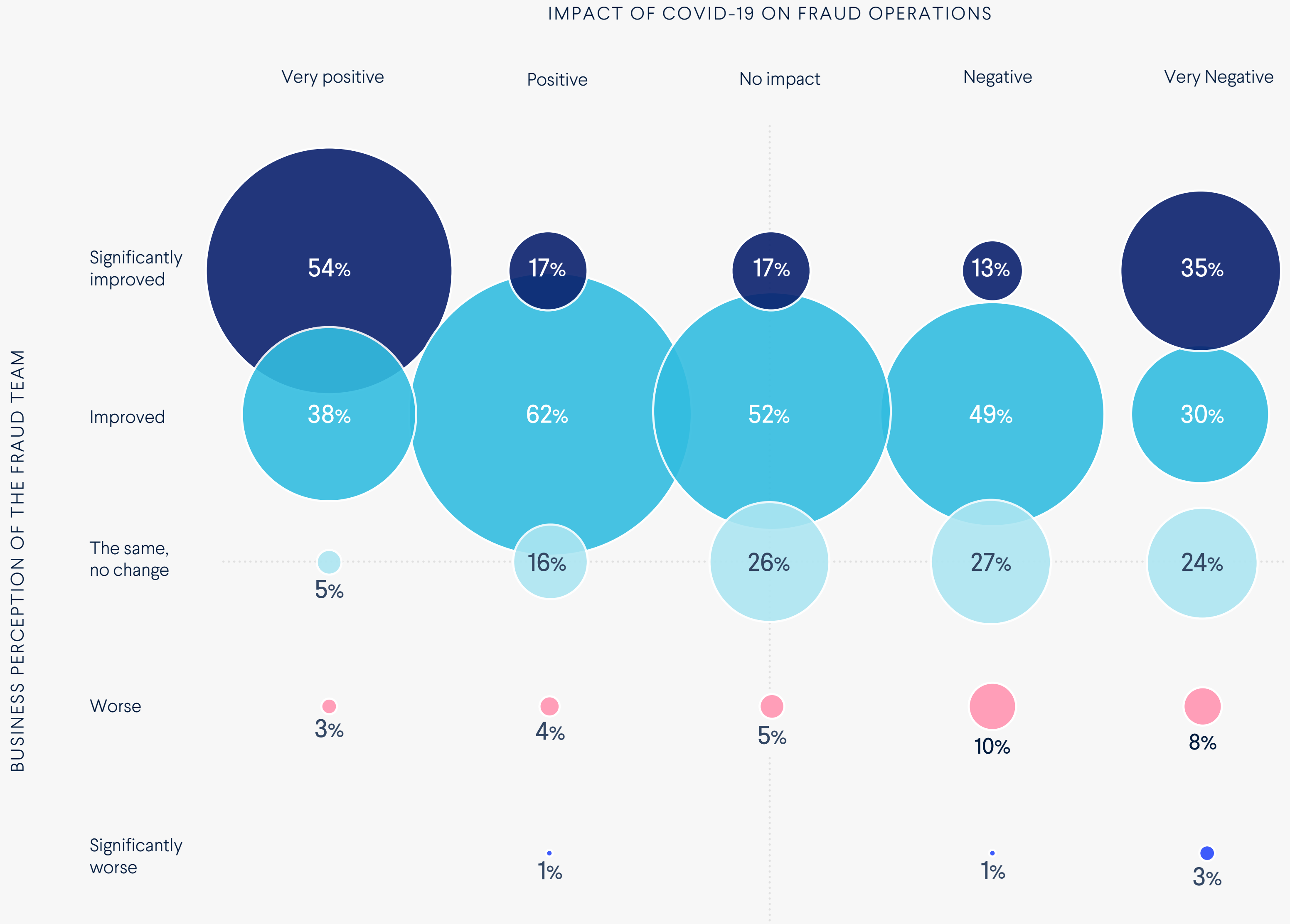
75%

**of participants report an improvement in the wider business perceptions of the fraud team in the past year.**

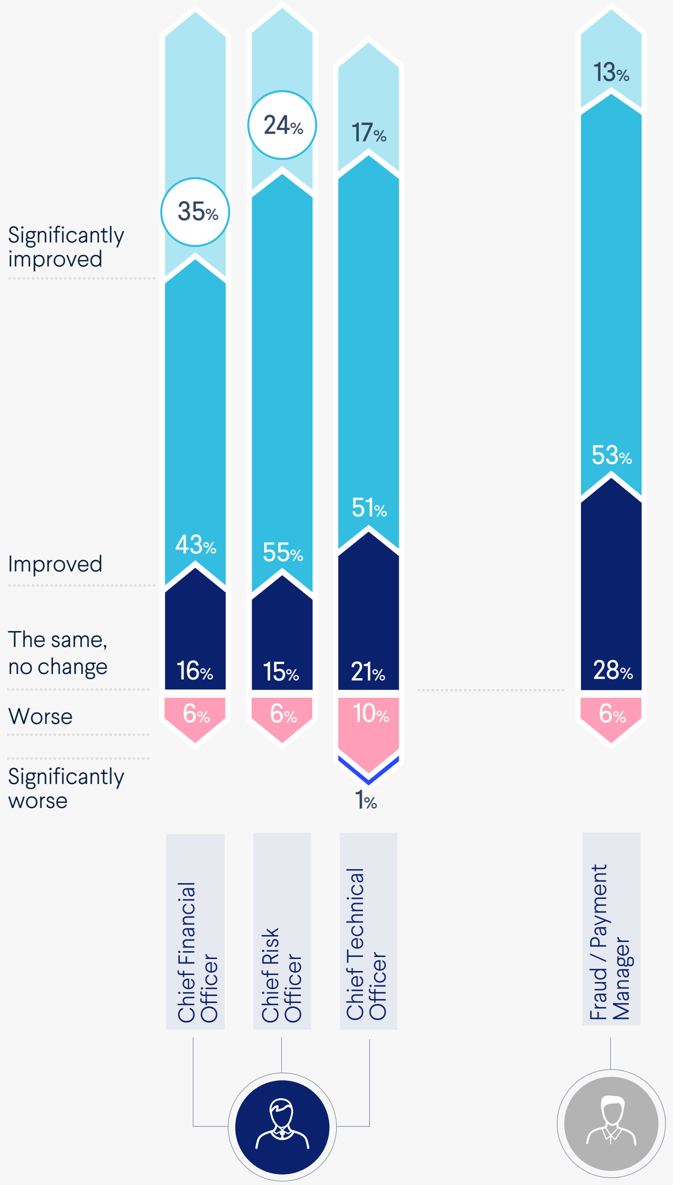
Senior roles are more likely to think that the fraud team is seen in a better light. At C-level almost 80% of CFOs, CROs and CTOs report an improvement, with over a third of CFOs reporting a significant improvement. This is really encouraging for fraud professionals who have been working hard to communicate the value of their team to the business.

However, Fraud Managers and Analysts are much less likely to think perception of the fraud team has improved significantly. This suggests that these teams may not be aware of how well they are doing and how valued they are.

## PERCEPTION OF FRAUD TEAM IN PAST 12 MONTHS **VERSUS THE IMPACT OF COVID-19 ON FRAUD OPERATIONS**

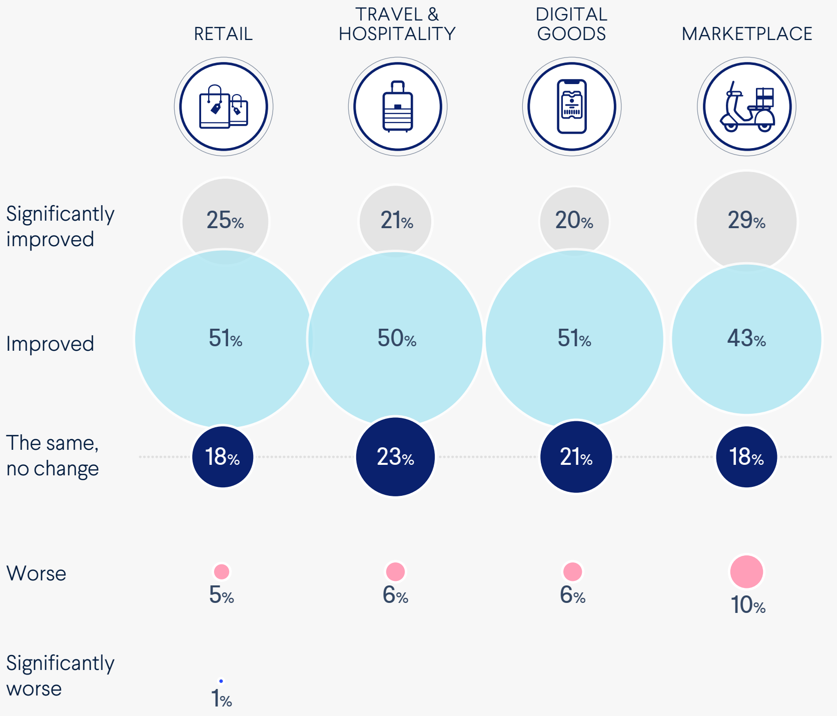


## PERCEPTION OF THE FRAUD TEAM BY JOB ROLE



Findings are similar across all industries, with the exception that 10% of Marketplace businesses report a more negative perception of the fraud team. Marketplaces are a relatively new concept and likely to be focused on high-growth, which can create some friction between growth and fraud teams. Despite this, Marketplace fraud teams are generally doing very well, with a majority (71%) saying their standing in the business has improved.

## PERCEPTION OF THE FRAUD TEAM BY INDUSTRY



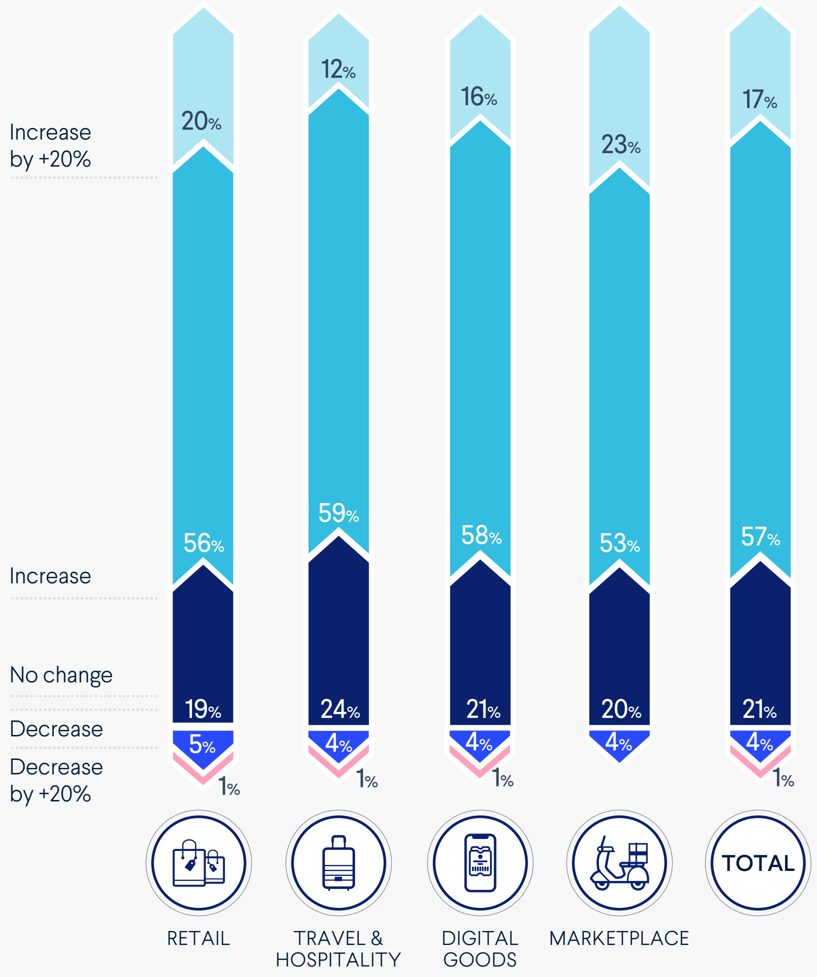
# 5.0 TOOLS & BUDGETS

## Fraud budget forecast in the next 12 months

Overall, 71% of all participants predict that their budget to tackle fraud will increase in the next 12 months. Of those who predicted a significant increase in their budget, 95% also predicted an increase in the size of their fraud team. This predicted budget increase may reflect the persistent and increasing sophistication of fraud and the threat it poses to merchant businesses. As we will see later on, many businesses have also reported a rise in multiple forms of fraud in the past 12 months.

**71%** Of all participants predict that their budget to tackle fraud will increase in the next 12 months.

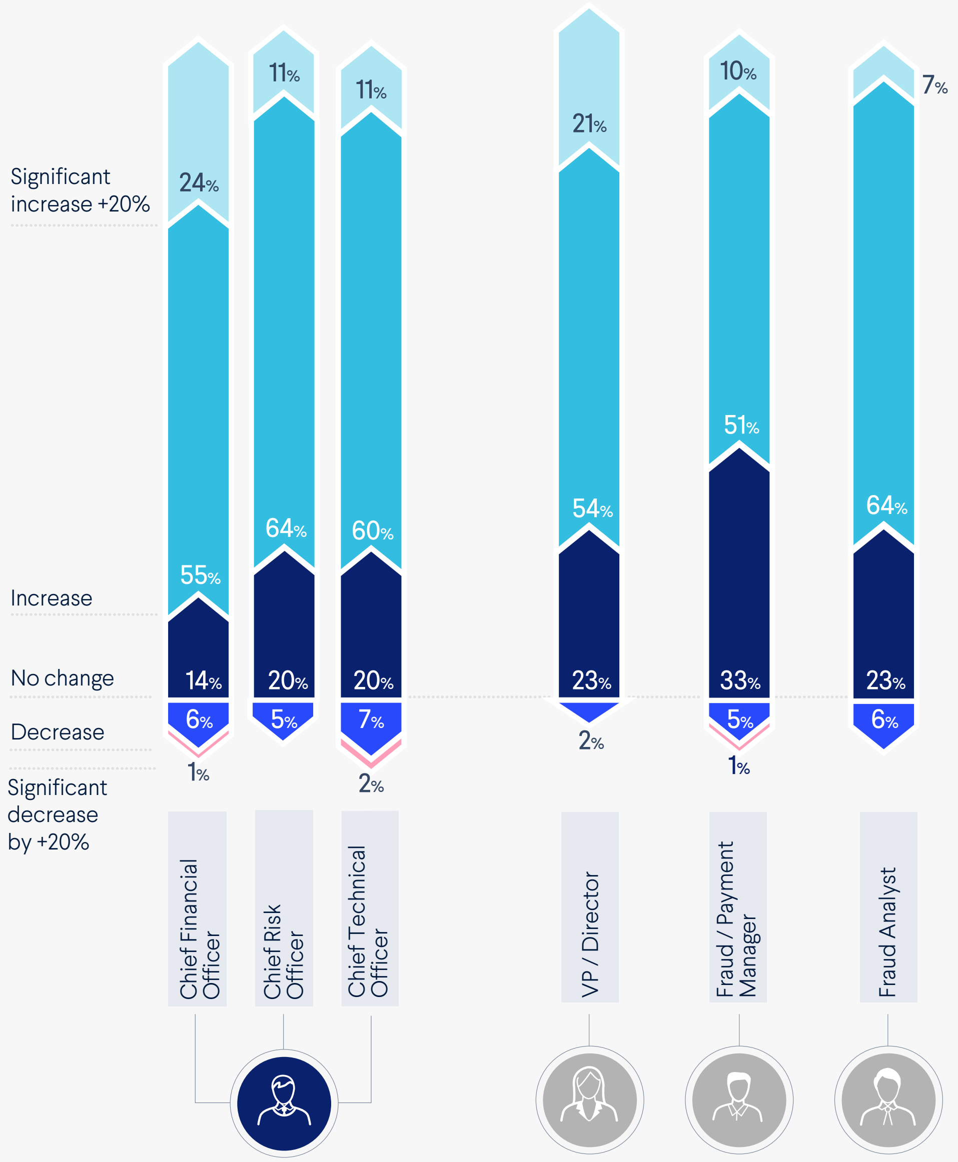
TOTAL FRAUD BUDGET PREDICTIONS **FOR THE NEXT 12 MONTHS** (TOOLS, FRAUD LOSS, STAFF)



Almost nine out of ten CFOs surveyed predict an increase in their business fraud budget – with almost a quarter predicting a significant increase. This contrasts with Fraud/Payments Managers, where 61% predict an increase in budget.

It's not surprising that CFOs would be more knowledgeable on financial forecasts, but perhaps this suggests that there hasn't been effective communication within business teams.

FRAUD BUDGET FORECAST IN THE NEXT 12 MONTHS
**BY JOB ROLE**



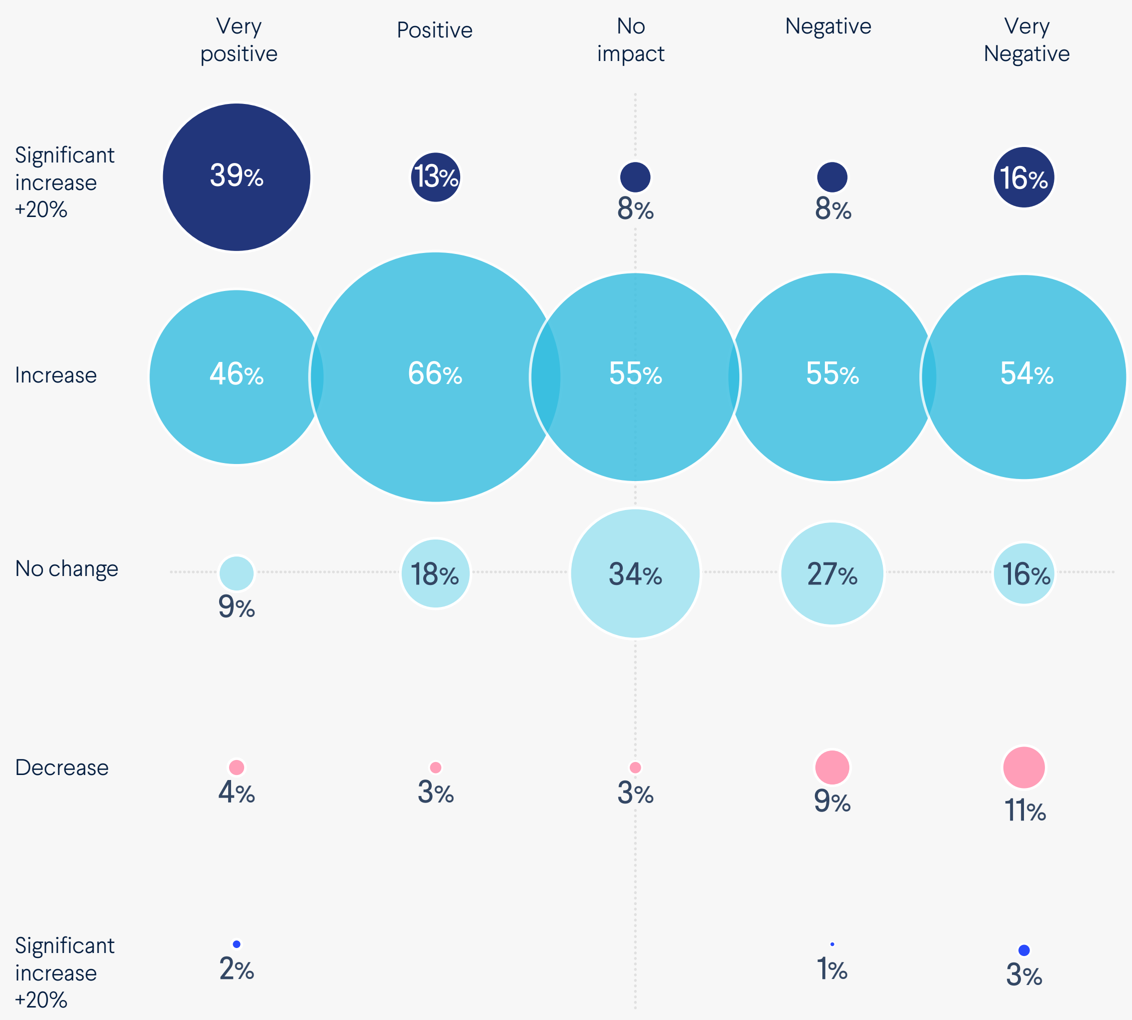
This could be partially explained by the impact of Covid-19. Respondents who said that Covid-19 has had a positive effect on their business fraud operations were more likely to predict an increase in their fraud budget.

## Why is Covid-19 seen as positive for fraud teams?

**We already know Covid-19 has caused a monumental rise in online transactions. This in turn can require a larger online fraud team or better resources to manage the increased risk of fraud, giving teams more budget.**

We also have evidence that Covid-19 outbreak has actually resulted in lower fraud in some businesses. An example is online groceries merchants - due to the huge surge in demand, many grocery businesses restricted orders to existing customers only. This has meant fraud levels have dropped significantly, while transaction levels and revenue has gone up. However, this can't continue, and these merchants need to prepare for when they open up to new customers again. This budget increase could be part of the contingency planning for when these restrictions are relaxed and the business is exposed to greater risks.

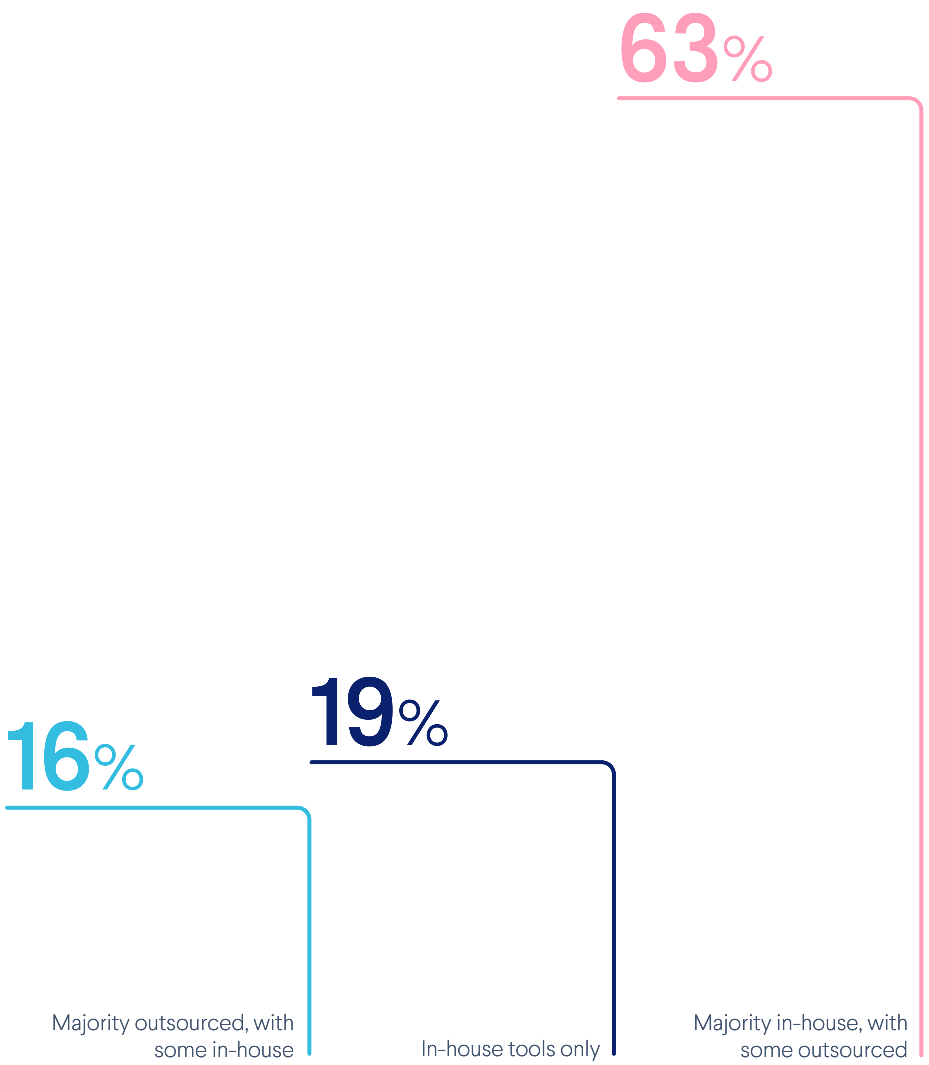
IMPACT OF COVID ON FRAUD **VERSUS** THE BUDGET FORECASTS FOR THE NEXT 12 MONTHS



# 5.1 TOOLS & BUDGETS

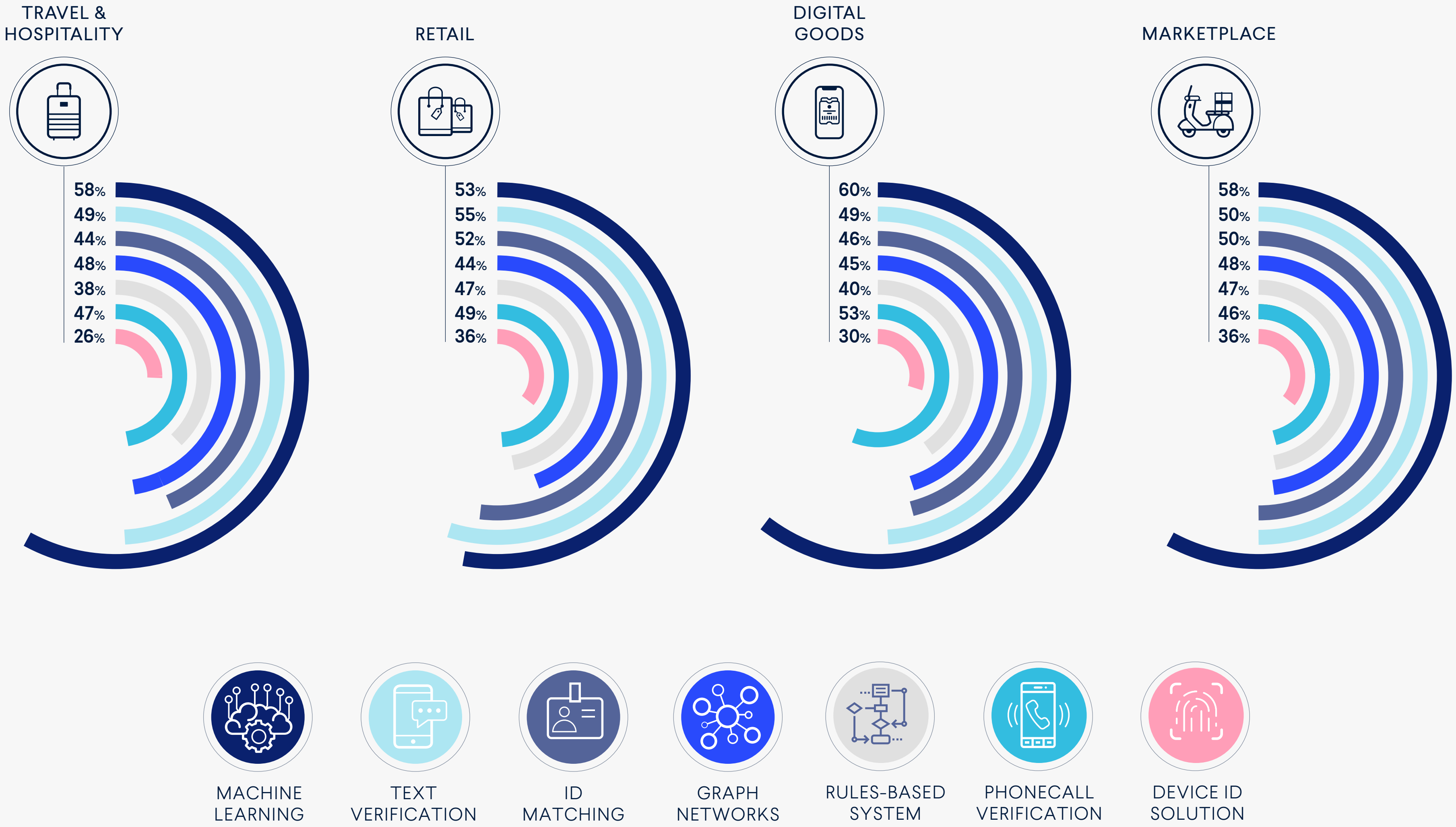
## TOOLS USED AGAINST FRAUD

Most businesses (79%) are using a mixture of in-house and outsourced tools against fraud. Almost one in five businesses are currently using in-house tools alone. A very small proportion (2%) are using outsourced tooling alone.



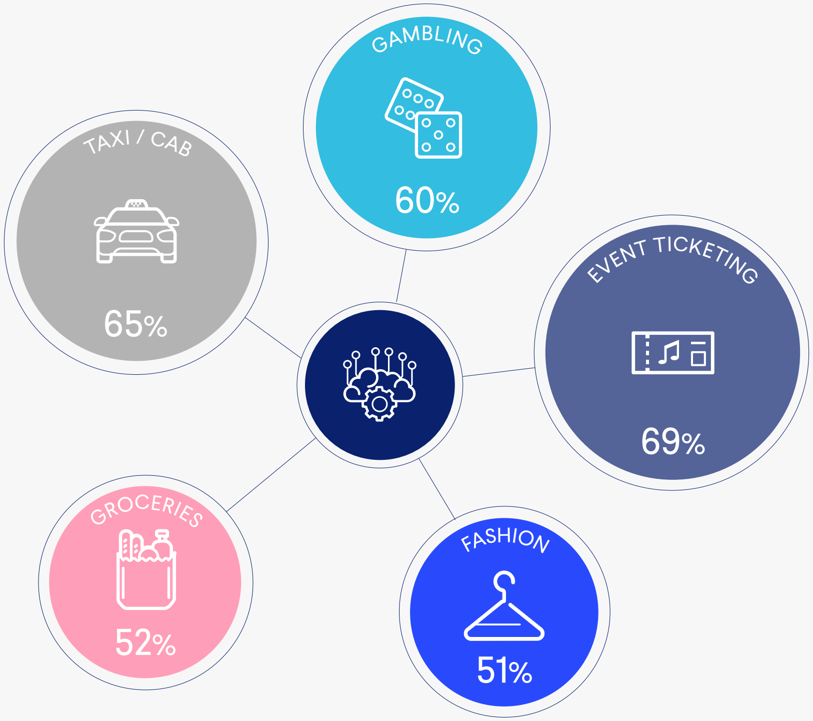
## TOOLS USED TO TACKLE FRAUD

Online businesses use a combination of different types of tools to tackle fraud rather than relying on one system. Over half of respondents in every industry are using some form of machine learning technology against fraud.



Machine learning methods are more likely to be used by Digital Goods and Marketplace merchants- in particular Taxi/Cab services, Gambling and Event Ticketing. Machine learning is less widely used in Retail - for example by Fashion and Groceries merchants.

MACHINE LEARNING INDUSTRIES



It's important to note that machine learning is a somewhat ambiguous term when used in relation to fraud detection - with multiple solution providers taking vastly different approaches to data use and a broad range of interpretations of the term.

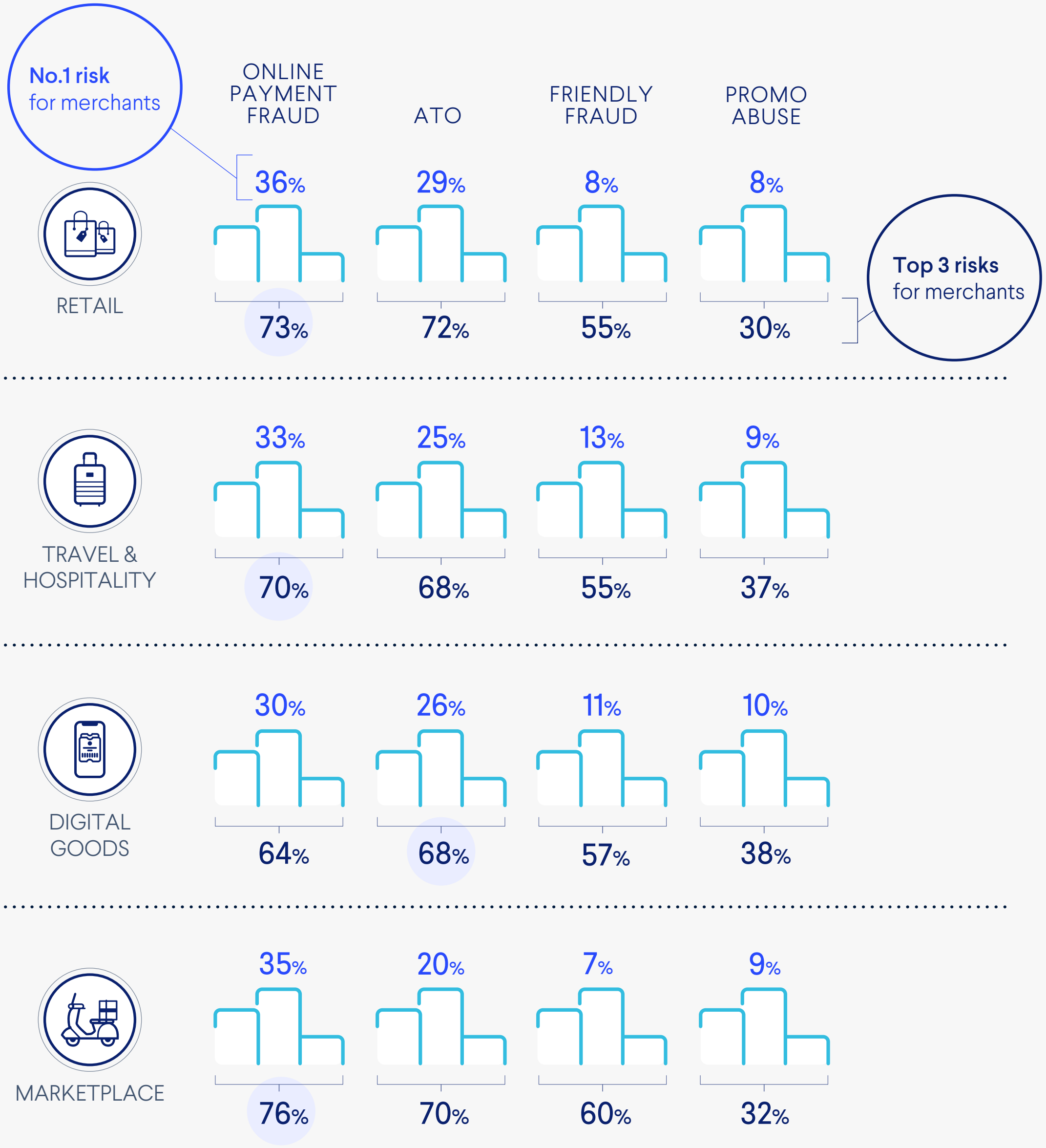
Relatively few merchants are using graph networks or a device ID solution which may be a concern when considered against the increasing rise in ATO attacks. Graph network use is more common in businesses with an immediate sale nature - for example Gambling (53%), Taxi/Cab services (52%) and Food delivery (47%), however there is a fairly low adoption rate of these technologies overall.

# 6.0 MONITORING FRAUD & TRENDS

## Top risks by fraud trend

Next we'll look at survey respondents' perceptions of different fraud types - in particular which types of fraud present the biggest risks to their business. We asked participants to rank fraud types according to the perceived risk. These diagrams show which fraud risks are perceived to be the biggest threats by merchants, and the percentage of merchants in each industry group that put each fraud type in the top three risk categories.

## INDUSTRY GROUP PERCEPTIONS OF THE HIGHEST FRAUD RISKS



It's no surprise that the top two fraud risks to merchants are online payment fraud and ATO. This is consistent across all the industry groups, with only minor variations.

Online payment fraud costs merchants more than any other form of fraud, and the costs are still rising. It was revealed at the **2019 CNP Expo** that for every $1 in fraud loss, the true cost to merchants is $3.13 - a 6.5% increase from the previous year.

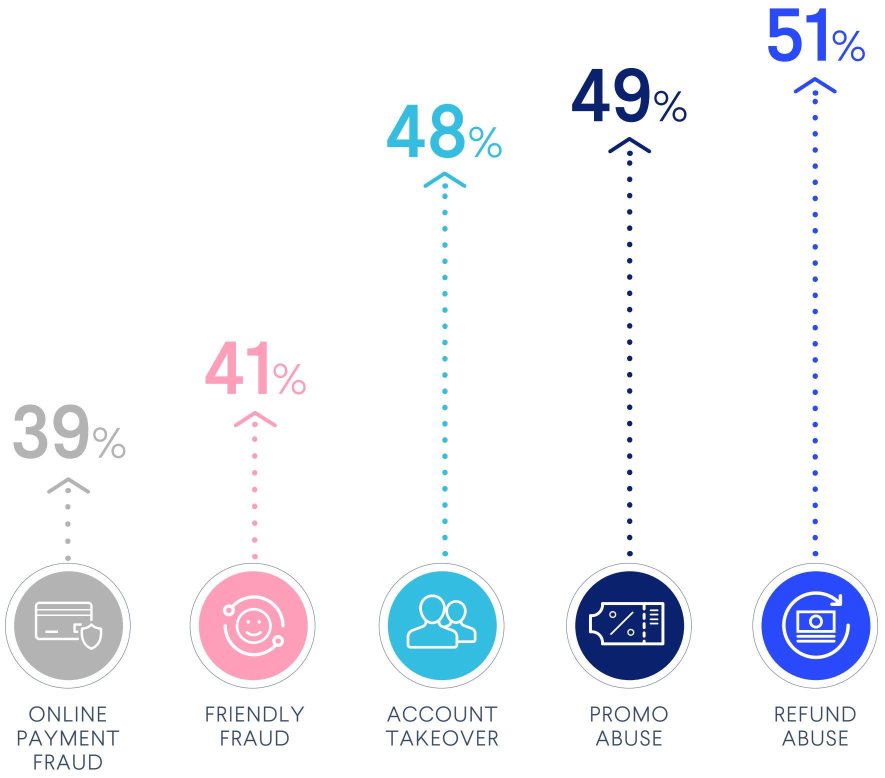
It's interesting to see that promotion abuse is perceived as one of the top risks for significant proportions of some business types. For example, promotion abuse was either a number one or number two concern for more than one in five businesses in the Marketplace and Travel & Hospitality sectors. For Digital Goods businesses, this was even higher, with over a quarter naming promotion abuse as a top level risk. As we will see later, this is also reflected in the growth of this activity in the previous 12 months.

# 6.1 MONITORING FRAUD & TRENDS

## Fraud levels in the past 12 months

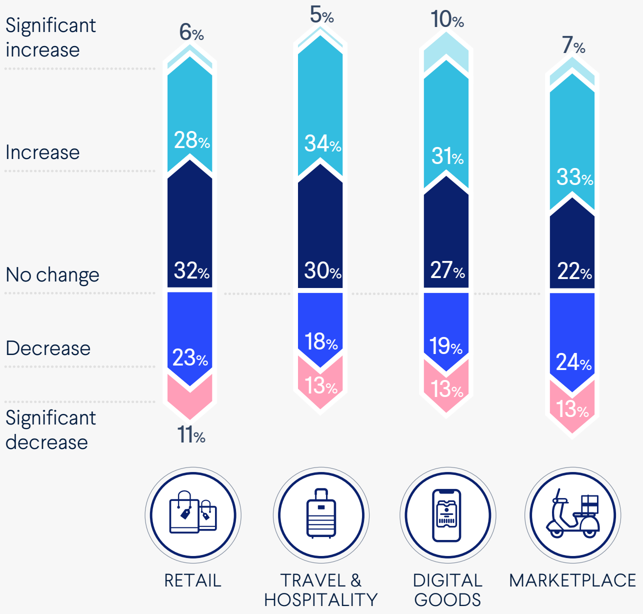
We asked survey participants about how fraud levels have changed in the past 12 months. Across all industries, the majority of businesses report increases in all the fraud types we asked about. We have seen that online payment fraud is still the number one concern for most businesses, however our results show that other forms of fraud are increasingly affecting a greater proportion of merchants.

PERCENTAGE OF MERCHANTS THAT EXPERIENCED
**AN INCREASE IN FRAUD ACTIVITY IN THE PAST 12 MONTHS**



## Online payment fraud increase in the past 12 months

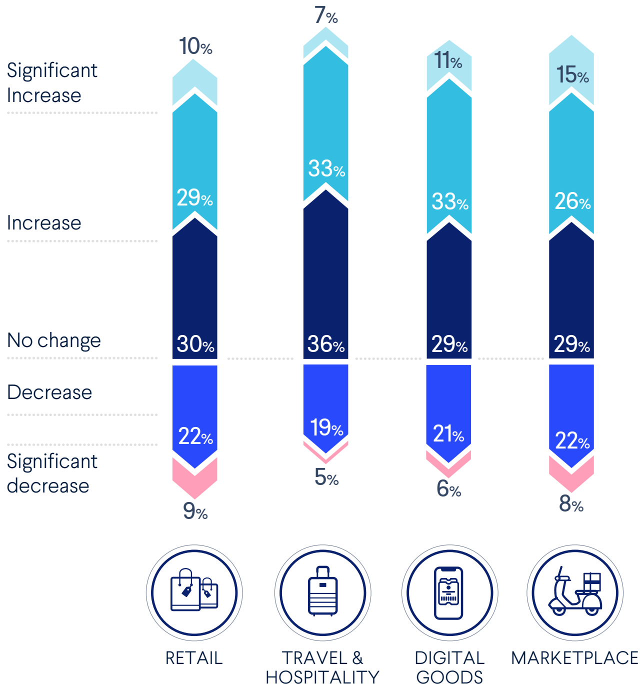
ONLINE PAYMENT FRAUD



It's interesting to note that even though overall 39% of merchants said that online payment fraud has increased in the past year, fewer Retail merchants said there has been an increase compared to the other business sectors. Even further, around a third of merchants in every sector said that online payment fraud has actually gone down in the past 12 months.

## Friendly fraud increase in the past 12 months

FRIENDLY FRAUD

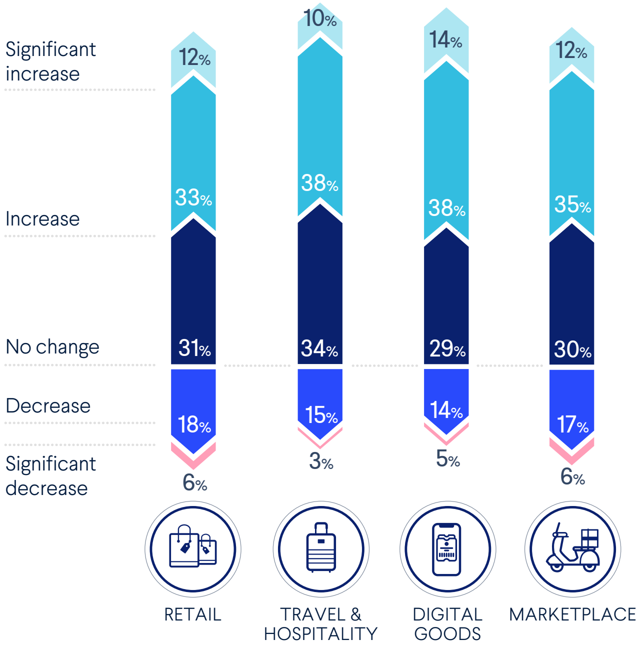


Friendly fraud, also known as first-party fraud, occurs when a customer makes a purchase with their own credit card, and then requests a chargeback instead of contacting the merchant for a refund. Around 40% of merchants say this form of fraud has increased, but like online payment fraud, up to a third of merchants in every industry group report a reduction in friendly fraud activity in the past year.

## Account takeover increase in the past 12 months

ATO attacks have increased for almost half of businesses surveyed, with over one in ten businesses reporting a significant increase in ATO activity. This is another indicator that ATO is the biggest risk to merchants after online payment fraud. Although some businesses report a decrease in ATO activity this is fewer than for online payment fraud or friendly fraud.

ATO ATTACKS



## Promotion abuse and refund abuse

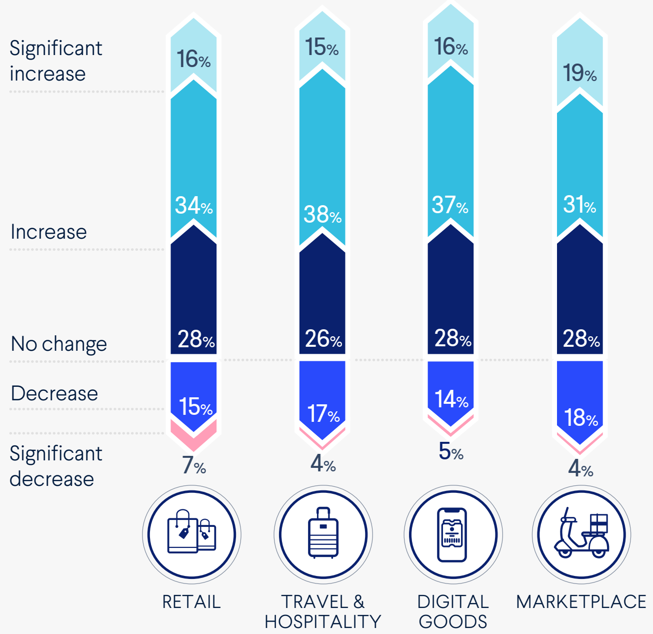
Both refund abuse and promotion abuse are increasing more than other forms of fraud, and these can cause huge losses for merchants.

It's easier than ever for customers to get refunds, and this brings challenges when opportunistic customers take advantage of terms and conditions. Due to Covid-19, many merchants have made refund policies more flexible, which brings more risks.

Merchants often offer promotions such as discount codes or referral codes during business expansion or in order to retain customers. However, it can be extremely difficult to track which customers are using them legitimately. Due to the nature of these codes, when they are being used at scale as they are intended to be, they can often hide the true losses.

## Refund abuse increase in the past 12 months

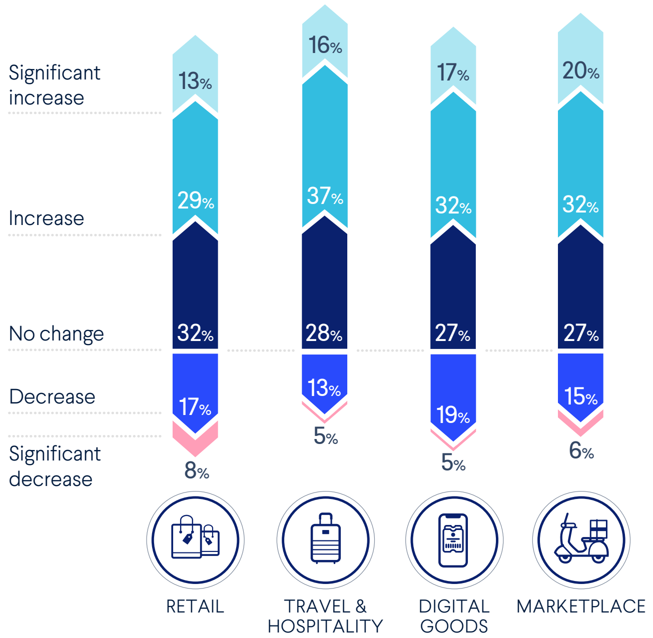
REFUND ABUSE



The significant rise in refund abuse across Retail and Marketplace sectors could be related to the rise in contactless delivery of goods. During the Covid-19 pandemic, many online retailers announced that delivery staff would leave products outside the customer's front door rather than ring the bell. This means the delivery may not be confirmed and the customer has the opportunity to claim that they never received the goods.

## Promotion abuse increase in the past 12 months

PROMOABUSE



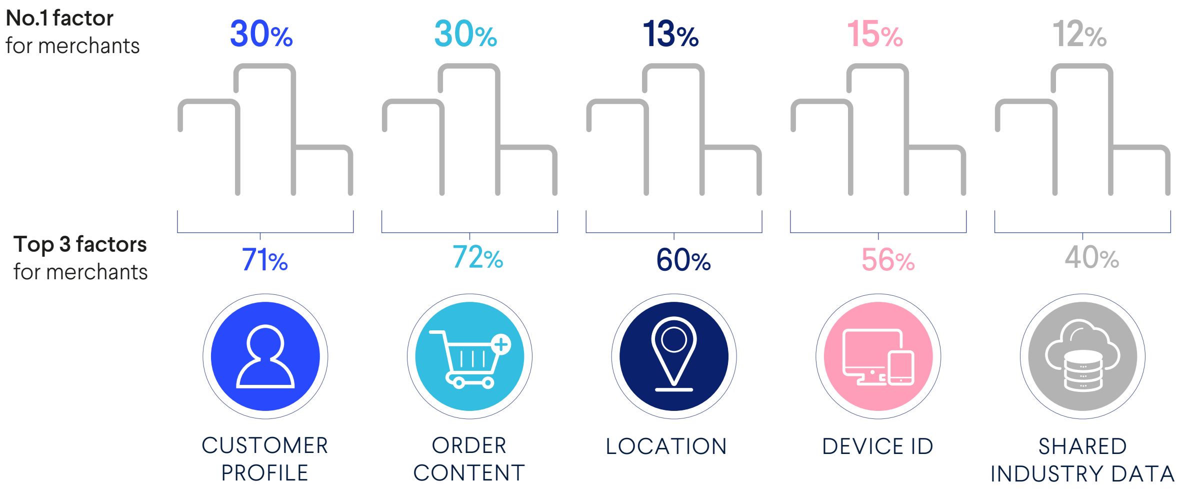
Promotion abuse has increased for a large proportion of merchants, second only to refund abuse. One in five Marketplace merchants has seen a significant increase in promotion abuse. Marketplaces are particularly likely to run promotions as they expand, and these businesses have also seen a significant rise in transactions due to the impact of Covid-19.

# 6.2 MONITORING FRAUD TRENDS

## Factors to identify fraud

We asked survey participants to rank the most important factors for identifying fraudulent orders. Across every industry group, the top factors are: the customer profile, order content, location data and device ID.

### TOP FACTORS FOR FRAUD



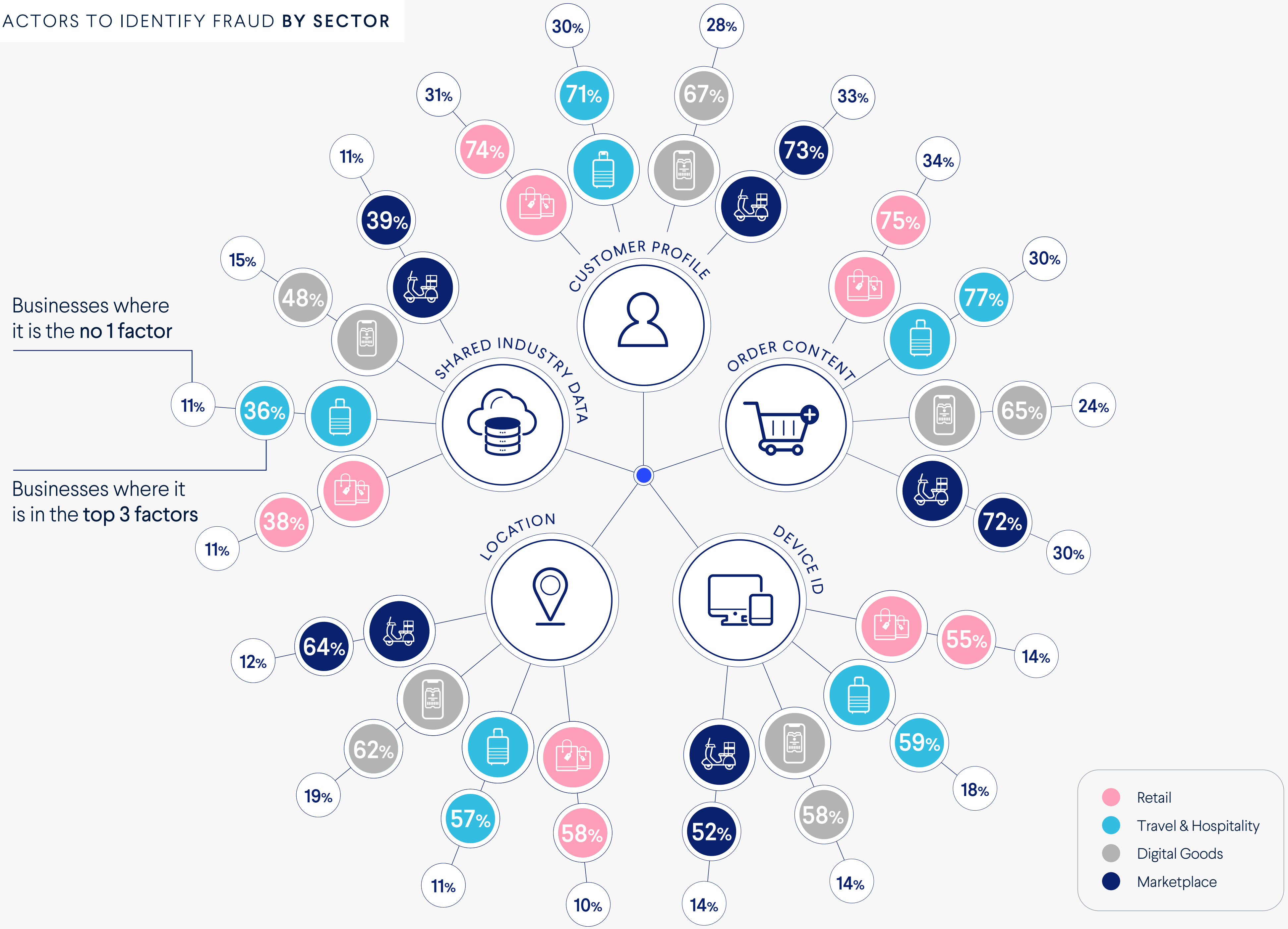
There are subtle variations between sectors. For example, in the Marketplace and Digital Goods industries, location data is seen as slightly more important, with 64% and 62% respectively naming location as one of the top three factors.

Additionally, order content is slightly more important to Retail businesses, with 34% naming it as the number one factor, compared to 30% in both Travel & Hospitality and Marketplaces and just 24% in Digital Goods. Location is seen as slightly less important by the Travel & Hospitality sector, with 57% naming it in the top three choices, behind Device ID with 59%.

Across all businesses, shared industry data is least likely to appear in the three most important factors, however it is still highly important for 40% of businesses. It's more common for Digital Goods businesses to see shared industry data as a key identifier. However, this difference is largely due to Gambling company responses, where 56% said shared industry data is in the top three factors, and 20% gave it the number one spot.

These subtle differences between wider industry sectors and even individual business types highlight how important it is for fraud solutions to be built around the business, rather than one size fits all.

## FACTORS TO IDENTIFY FRAUD **BY SECTOR**



Businesses where it is the **no 1 factor**

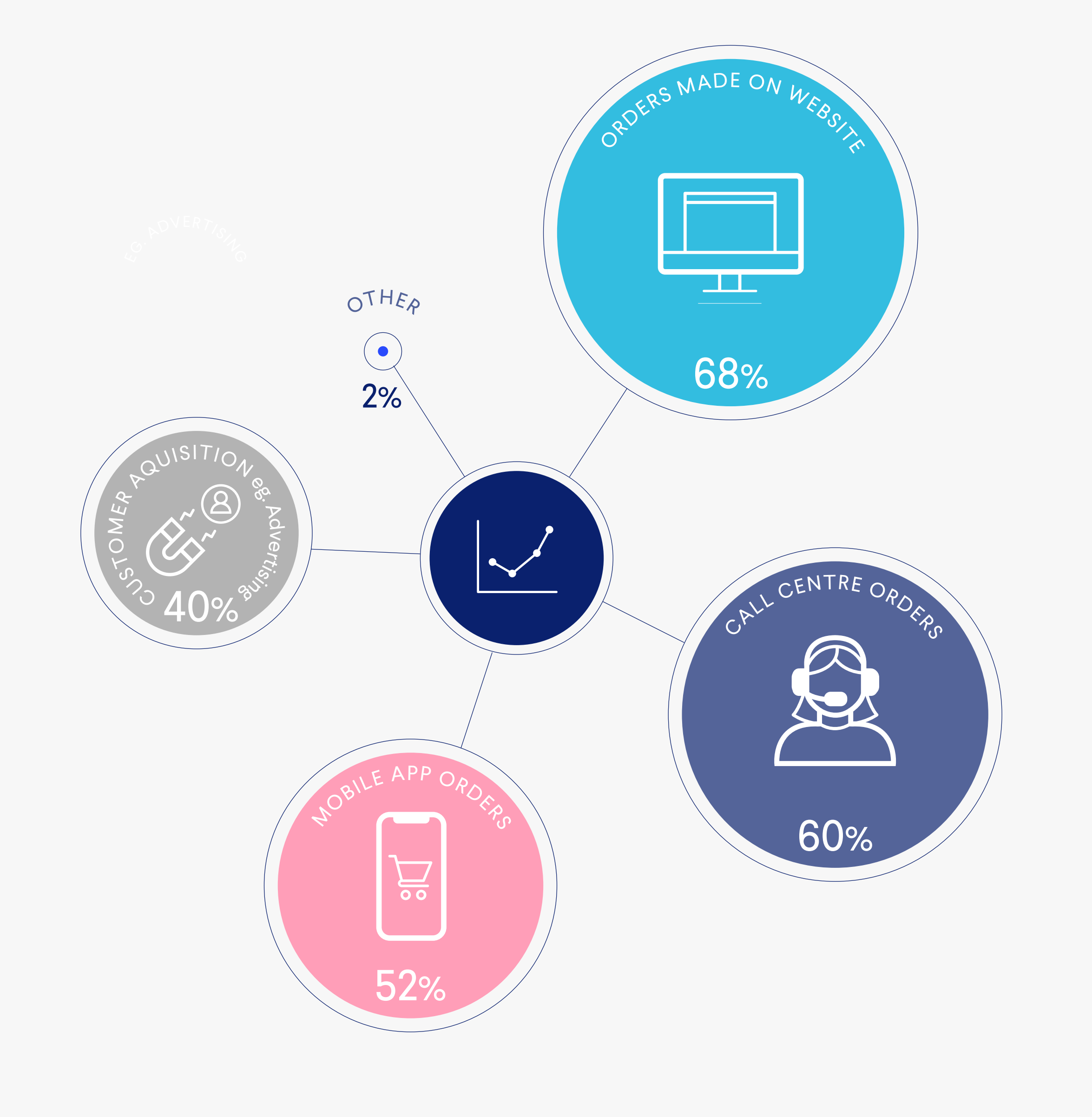
Businesses where it is in the **top 3 factors**

# 6.3 MONITORING FRAUD & TRENDS

Tracking fraud

We asked participants if they track the fraud percentages and general trends according to the below factors. Undoubtedly, the responses largely depend on individual business operations, and their customers' preferred way of ordering. For example, some businesses may not have a fully functional mobile app and/or a call center.

## TRACKING FRAUD **BY SPECIFIC DATA**



Most businesses are tracking fraud levels for orders made on the website (70%) with fewer numbers tracking orders made through call centres, mobile applications and the route of customer acquisition. More businesses are tracking fraudulent orders made via the call centre than are tracking mobile orders, which may be due to slower digitalization in some industries. As more and more transactions move online faster due to Covid-19, this is likely to force many companies to embrace digitalization faster.

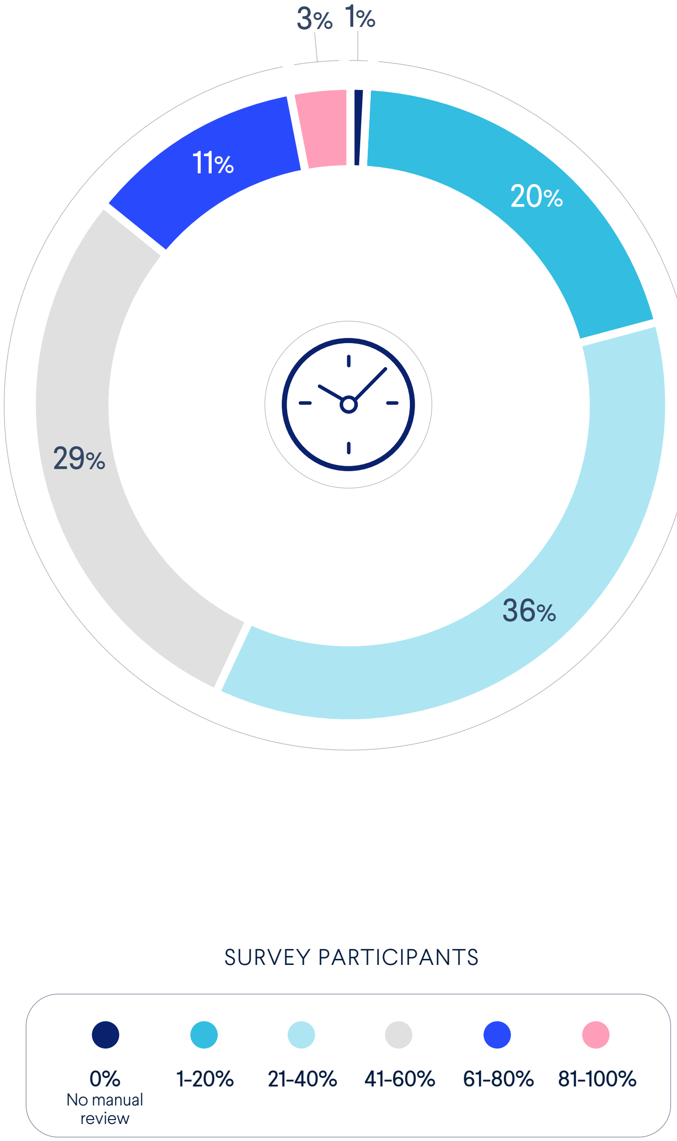
Marketplace businesses are far more likely to rely on mobile apps and also more likely to track fraud for mobile orders - for example, with 61% of Taxi/cab businesses and 62% of Product/Service delivery.

It's interesting to see that 40% of businesses are tracking fraud according to the customer acquisition route. Again, this is very dependent on the individual business type, as some traditional marketing acquisition routes are impossible to track, such as billboards or print advertising. Of the companies tracking fraud by the customer acquisition route, 43% said that promotion abuse has increased in the past 12 months. If this trend continues, we might see more online businesses looking at fraud by acquisition route to try and determine the cost of running marketing promotions.

# 7.0 MANUAL REVIEW

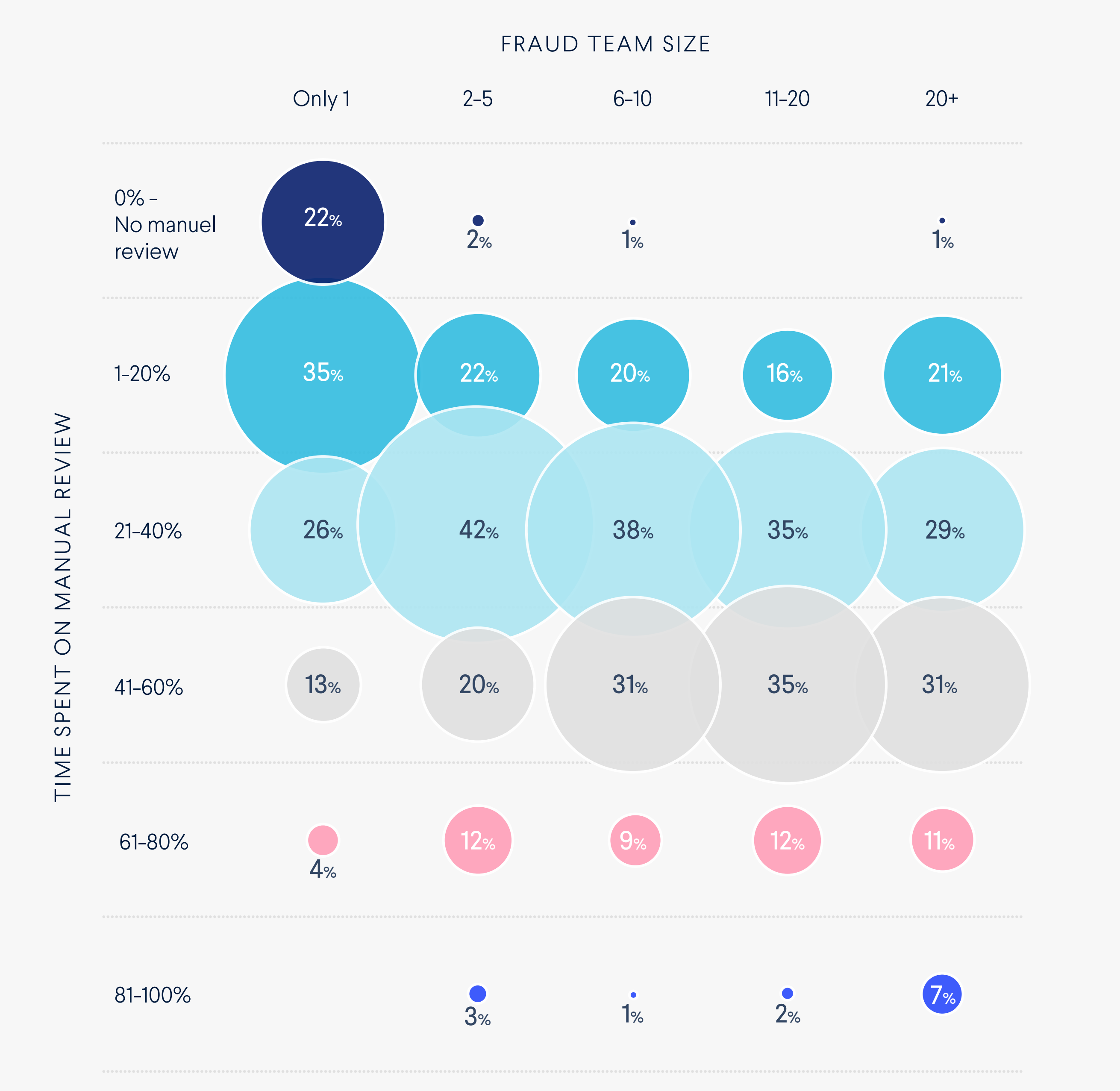
## Time spent on manual review

Overall, two-thirds of survey participants said their fraud team is spending between 20-60% of their time on manual review. This is the case even in larger fraud teams of 20+.



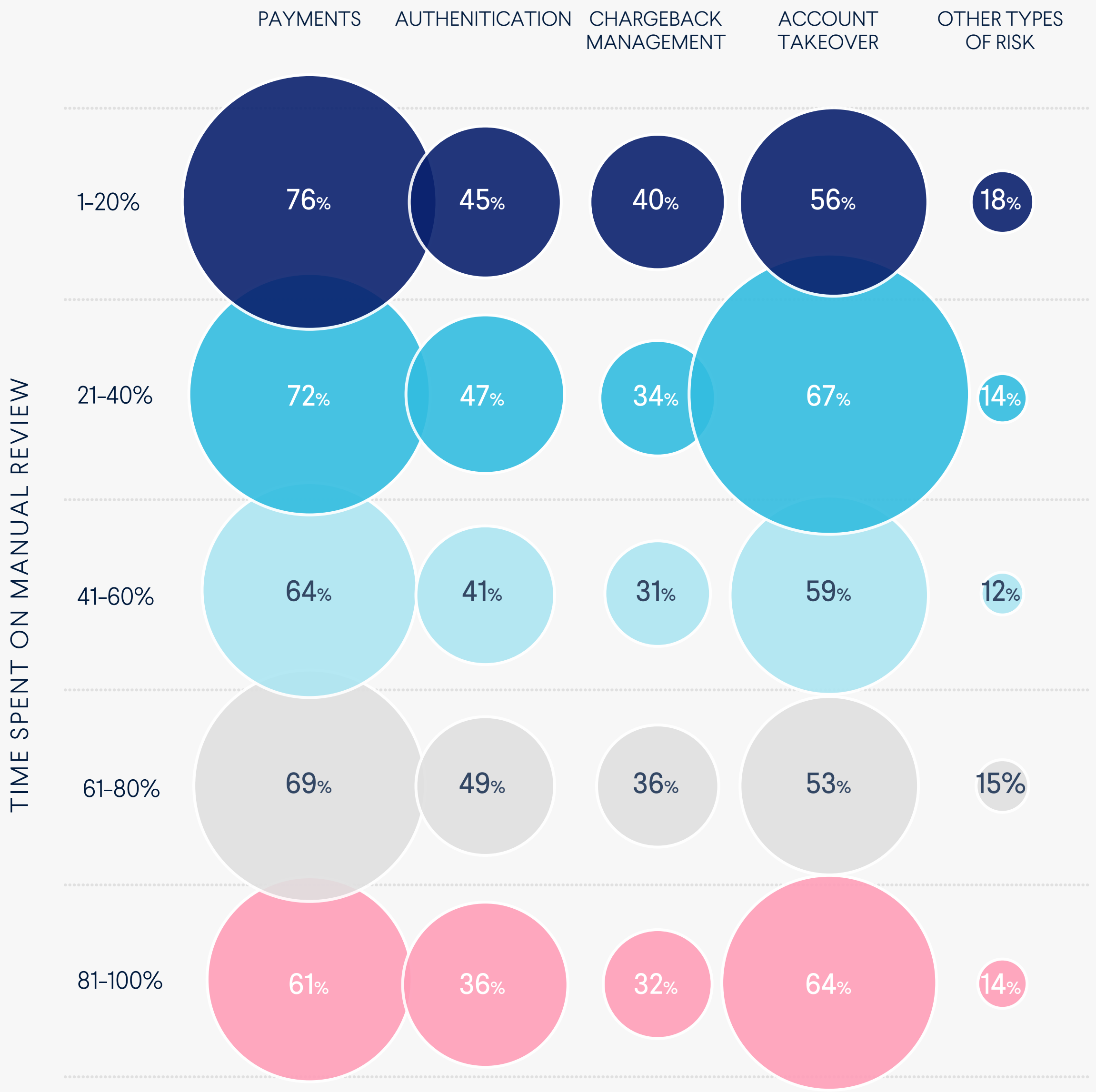
Even with the advances in fraud solutions, there is still a role for manual review - as shown by the amount of time dedicated to this. The exception is in some very small fraud teams (one person only) where they are not doing any manual reviews at all - perhaps because it's not possible, or the business has a fully automated outsourced fraud system.

TIME SPENT ON MANUAL REVIEW AND **FRAUD TEAM SIZE**



Smaller fraud teams tend to spend less time on manual review, which could be because the business has fewer transactions to review. This could also be due to the team having other responsibilities which take up their time. Shown below, teams that spend less than 20% of their time on manual review are more likely to manage payments, authentication and chargeback management than teams that spend over 81% of their time on manual review.

## AVERAGE TIME SPENT ON MANUAL REVIEW VS **FRAUD TEAM RESPONSIBILITIES**

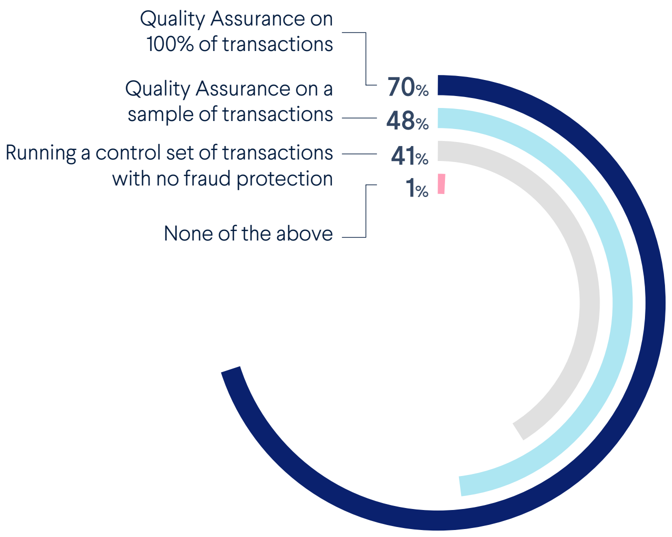


# 7.1 FALSE POSITIVES

## Measuring false positives

We asked participants about all the methods they have used or currently use to measure false positives. Overall, 70% of businesses have run Quality Assurance (QA) on 100% of their transactions. Almost half conduct QA on a sample of transactions, which suggests there is some overlap with those who QA 100% of transactions. This could suggest that merchants are not running QA on 100% of transactions 100% of the time, and this is a flexible strategy.

**METHODS TO MEASURE** FALSE POSITIVES (MULTIPLE-CHOICE)



**Surprisingly, 41% or merchants have run a control set of transactions with no fraud protection in place.**

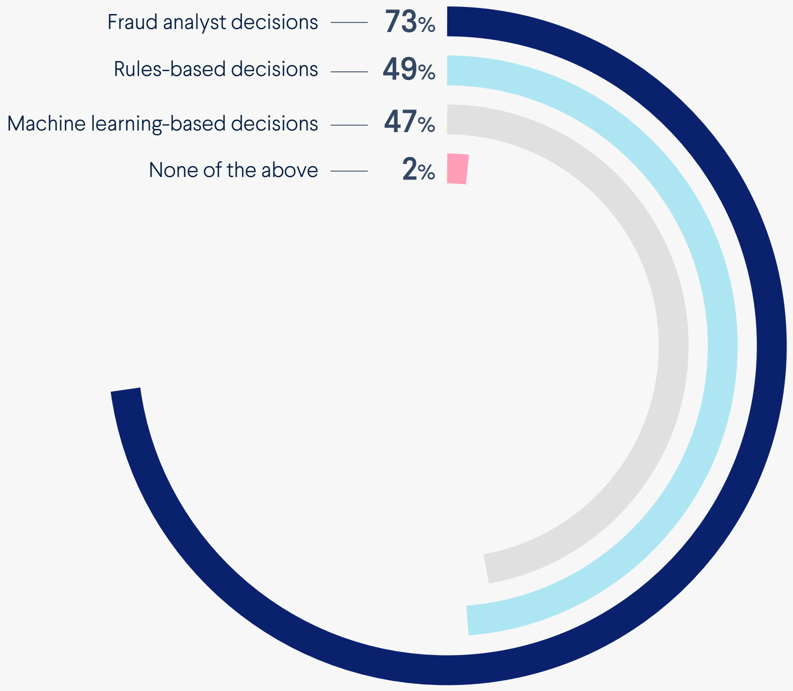
This is a high risk activity which could be very costly to the business. However, we don't have further information about the size of the control set, or whether this is a consistent control set or a sporadic test under certain conditions. Only 1% of businesses are not using any methods to measure false positives at all.

Next we asked the participants which fraud decisions are most likely to be reviewed to measure false positives. Almost three quarters say they review decisions made by a Fraud Analyst, while less than half review decisions made by rule-based systems or machine learning systems.

Could this be an indicator that businesses put more trust in tools than their team? Maybe not. It's likely that Fraud Analyst are making decisions on the more ambiguous cases, eg. the transactions where the fraud system has flagged these as needing human insight. It makes sense that these decisions would be reviewed in order to learn more about the ambiguous cases and take further insights for future similar transactions.

Additionally, not all the merchants included in this survey are using machine learning tools to fight fraud, and therefore they cannot review these decisions at all.

## DECISIONS ARE REVIEWED FOR FALSE POSITIVES

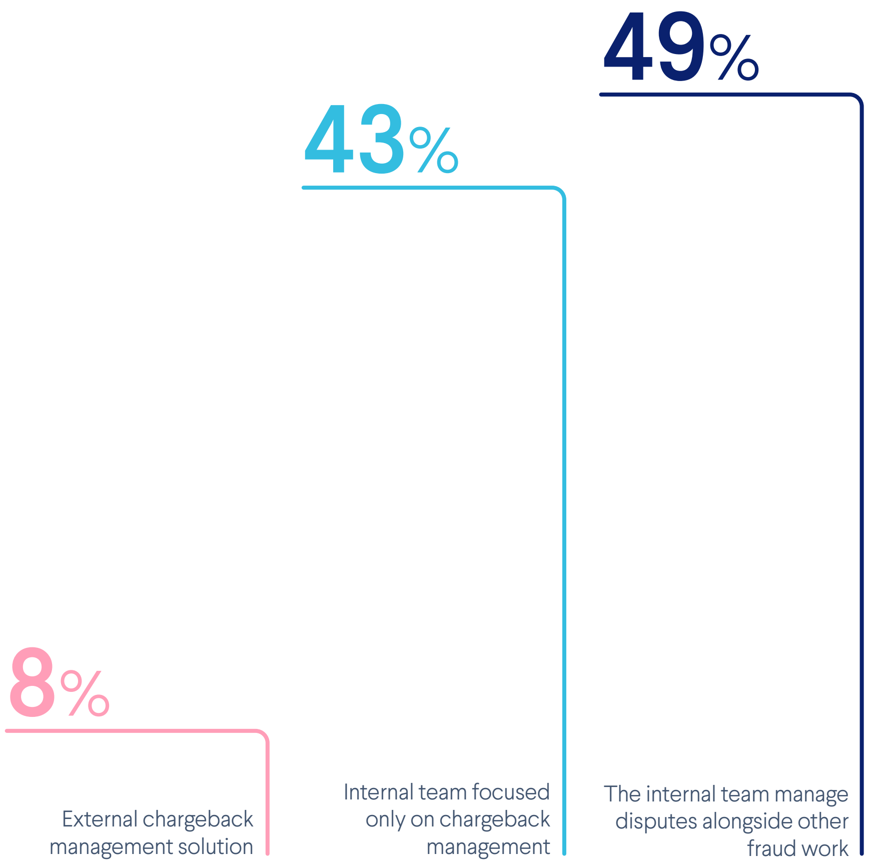


# 8.0 CHARGEBACK MANAGEMENT

## Chargeback management options

The majority of businesses we surveyed are managing their chargebacks internally, either in the fraud team or in a dedicated chargeback management team. Overall, 8% are using an external chargeback management solution.

CHARGEBACK OPTIONS



**56%**

**On average, companies challenge 37% of chargebacks, and are successful in 56% of challenges.**

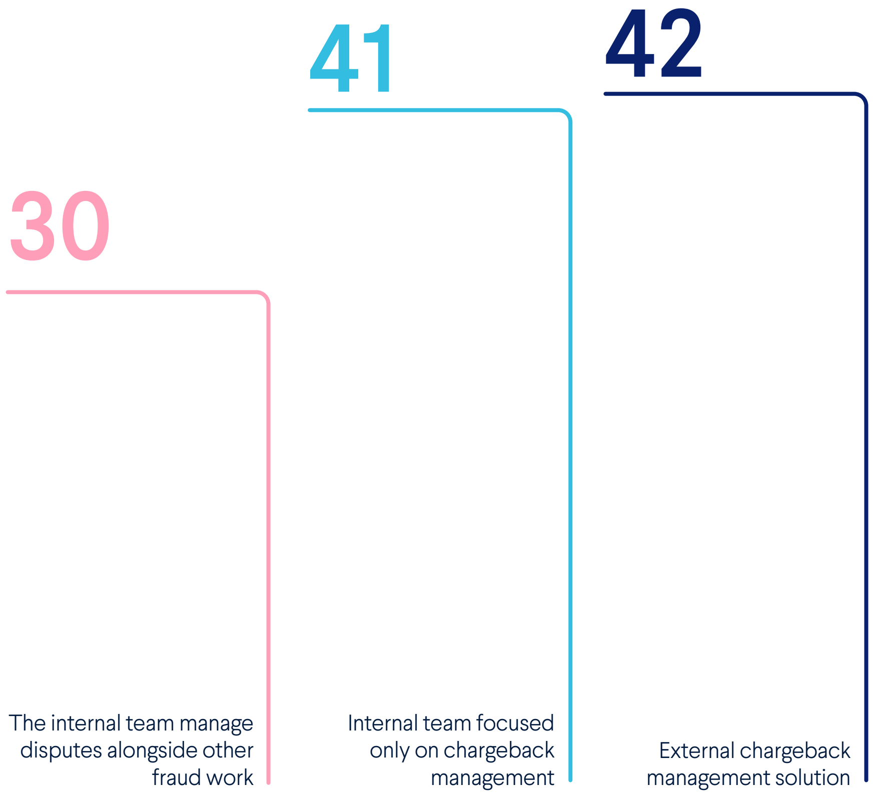
# 8.1 CHARGEBACK MANAGEMENT

## Chargeback challenge success

We looked at the challenge rate and success rate according to how the business manages chargebacks. Companies with either an internal or external team dedicated to managing chargebacks are likely to challenge significantly more chargebacks than companies where the fraud team is responsible for this as part of a wider scope of work.

### CHARGEBACK MANAGEMENT AND CHALLENGE RATE

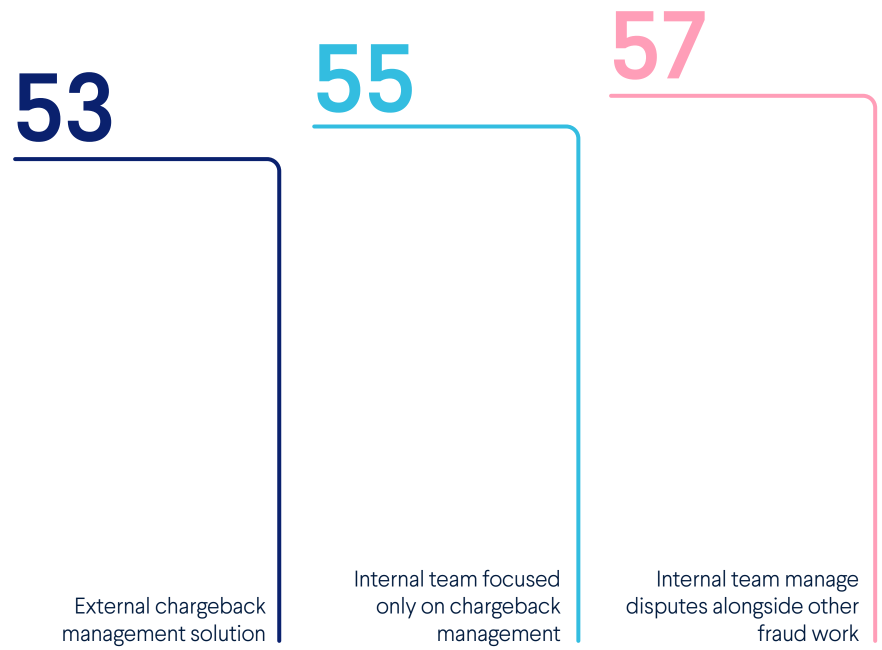
Median measurement



There was not a significant difference in challenge success rate between merchants where this is managed by the internal fraud team, a dedicated chargeback team or an external solution.

## CHALLENGE SUCCESS RATE AND CHARGEBACK MANAGEMENT METHOD

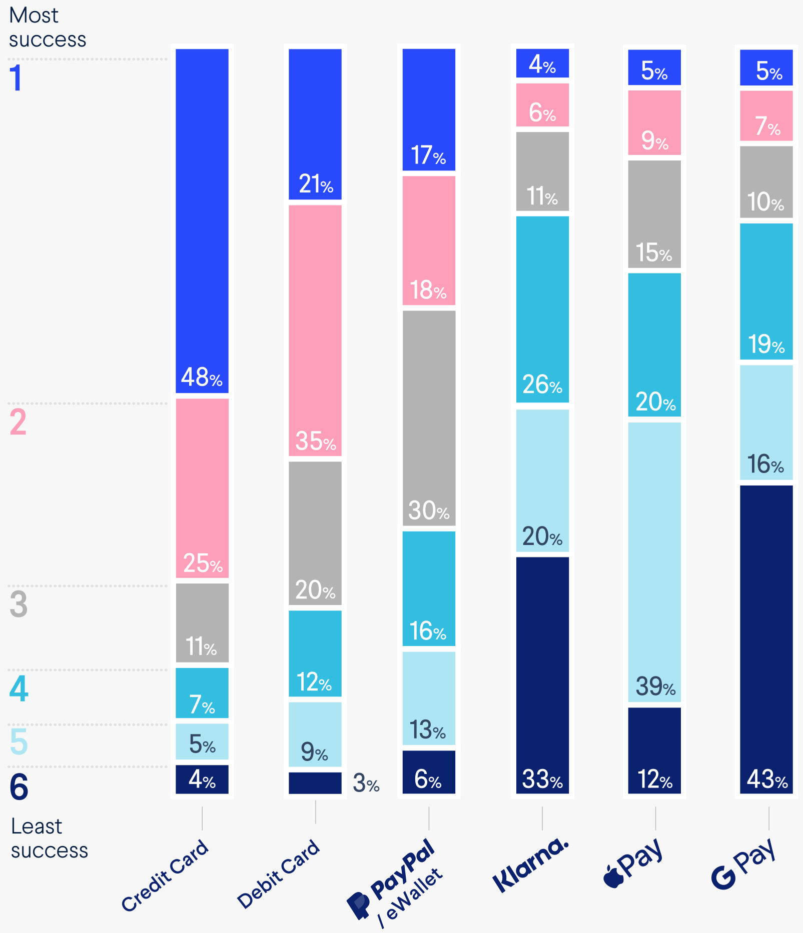
Median measurement



Businesses report that they have the most success when challenging credit/debit card chargebacks. Chargeback challenges on alternative payments like Klarna, ApplePay and GooglePay are least likely to be successful.

GooglePay in particular is seen as the most difficult payment method to challenge chargebacks, **despite GooglePay stating that chargebacks are dealt with in the same way as credit/debit cards.** Why could this be? It may be partly due to the inherent biometric authentication methods used by GooglePay/ApplePay.

## CHALLENGING CHARGEBACKS SUCCESS BY PAYMENT METHOD



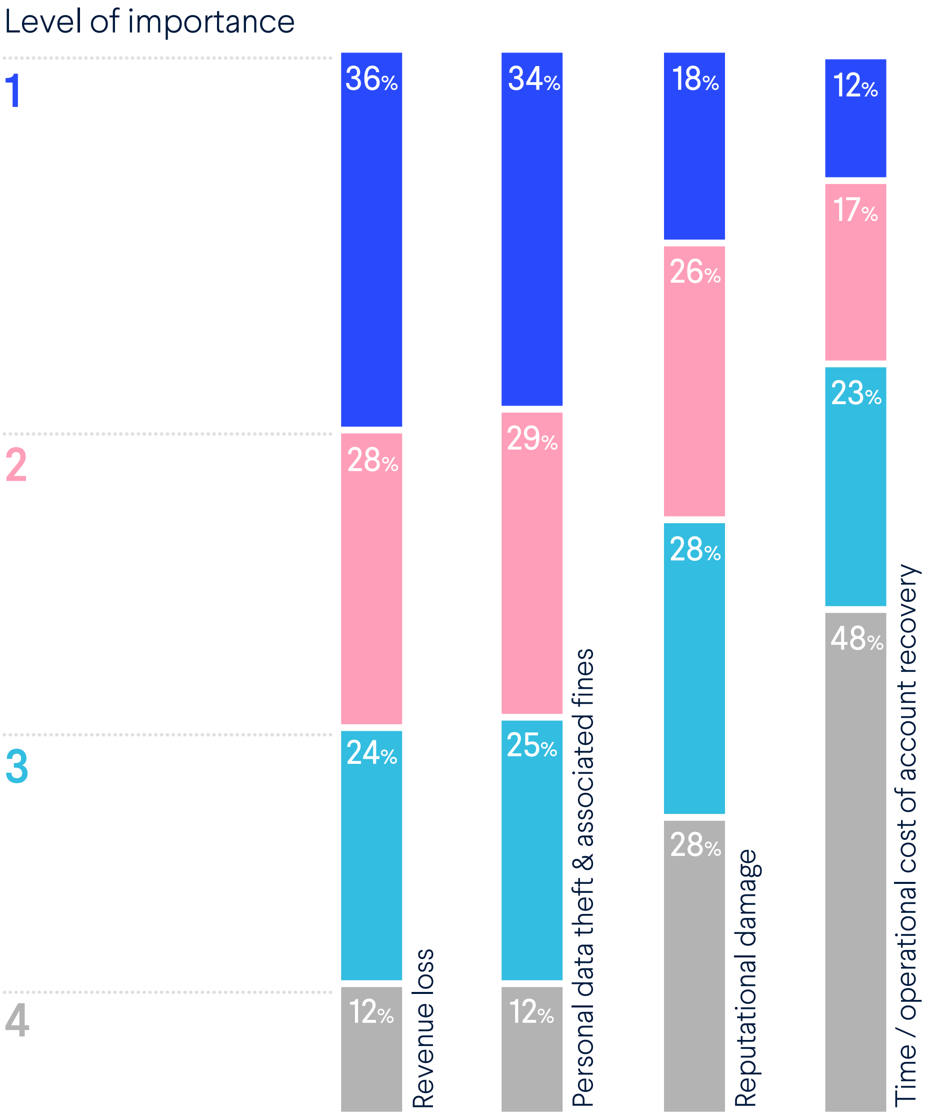
# 9.0 ACCOUNT TAKEOVER

## Business risks and dedicated tools

Account takeover has already been highlighted as a top risk, and over half the merchants said that it has increased in the past year alone.

We asked participants about the consequences of account takeover and severity of risk they pose. The top concerns for merchants are revenue loss and personal data theft and associated fines, with reputational damage a secondary risk. Even fewer businesses see the team operational costs as the most pressing concern.

This makes sense as it can be difficult to quantify these more intangible costs. For example, how can a business measure exactly how much its business reputation has suffered and what that costs? Or how much time and effort does it cost for their team to contact all customers with blocked accounts and reactivate them effectively? Plus, often these after effects of an attack can take a long time to be fully understood.



Overall, 83% of businesses have a tool specifically targeted at detecting and preventing account takeover, leaving around one in six businesses with no specific protection. Within those without account takeover tools, 47% named account takeover as the top three fraud risks to their business, and 28% said it has increased in the past year.

**Almost nine in ten (89%) of merchants say they are checking a breached credential database for customer login details.**

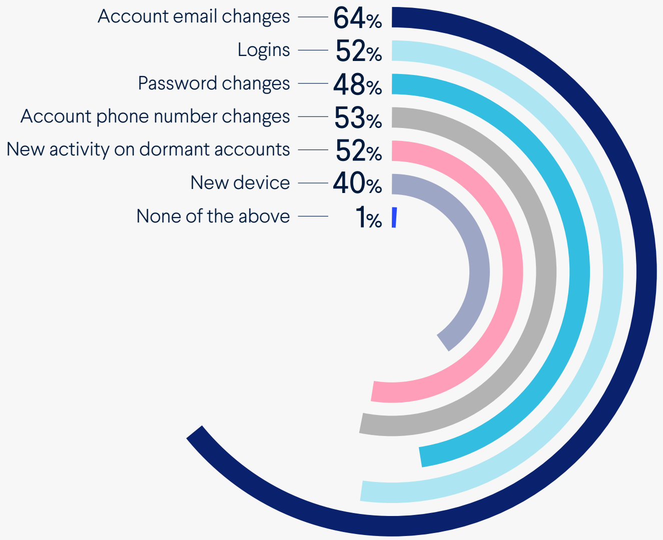
# 9.1 ACCOUNT TAKEOVER

## Customer activity monitoring

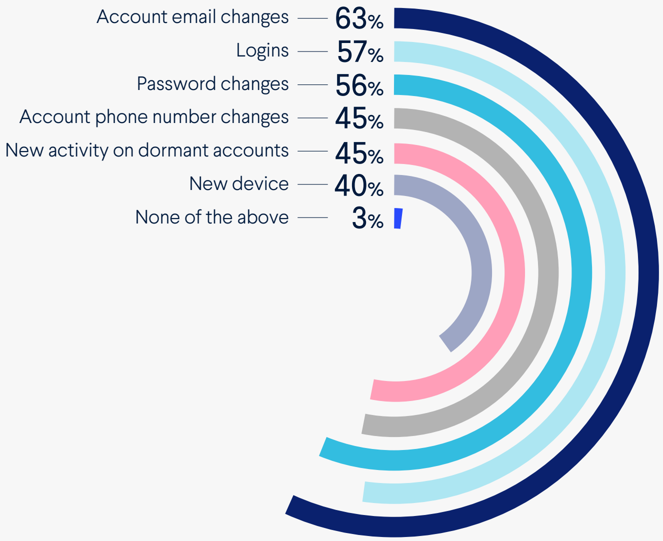
We asked respondents about which types of customer activity they monitor. There's little difference between activity monitoring between merchants with account takeover tools and those without. In fact, there were even more merchants without tools monitoring logins and password changes.

Relatively few merchants are monitoring customer activity which is key to detecting and preventing account takeover. It's particularly surprising to see how few merchants are monitoring customer logins and new devices on accounts, as these are the first point where any account takeover could be seen.

## WITH ATO TOOLS



## WITHOUT ATO TOOLS



# 48%

**Attackers changed the phone number after they successfully compromised an account.**

Tracking customer activities enables merchants to identify fraudster behavioral patterns. In our analysis of **account takeovers** on food delivery businesses, we found that 48% of attackers changed the phone number after they successfully compromised an account. Like any fraud, account takeover methods are often specific to the merchant and attackers targeting other sectors may do something different. Ultimately, people are creatures of habit, and even the most sophisticated fraudsters will repeat the same actions or patterns subconsciously. The key to catching them and protecting your business is to understand how they operate.

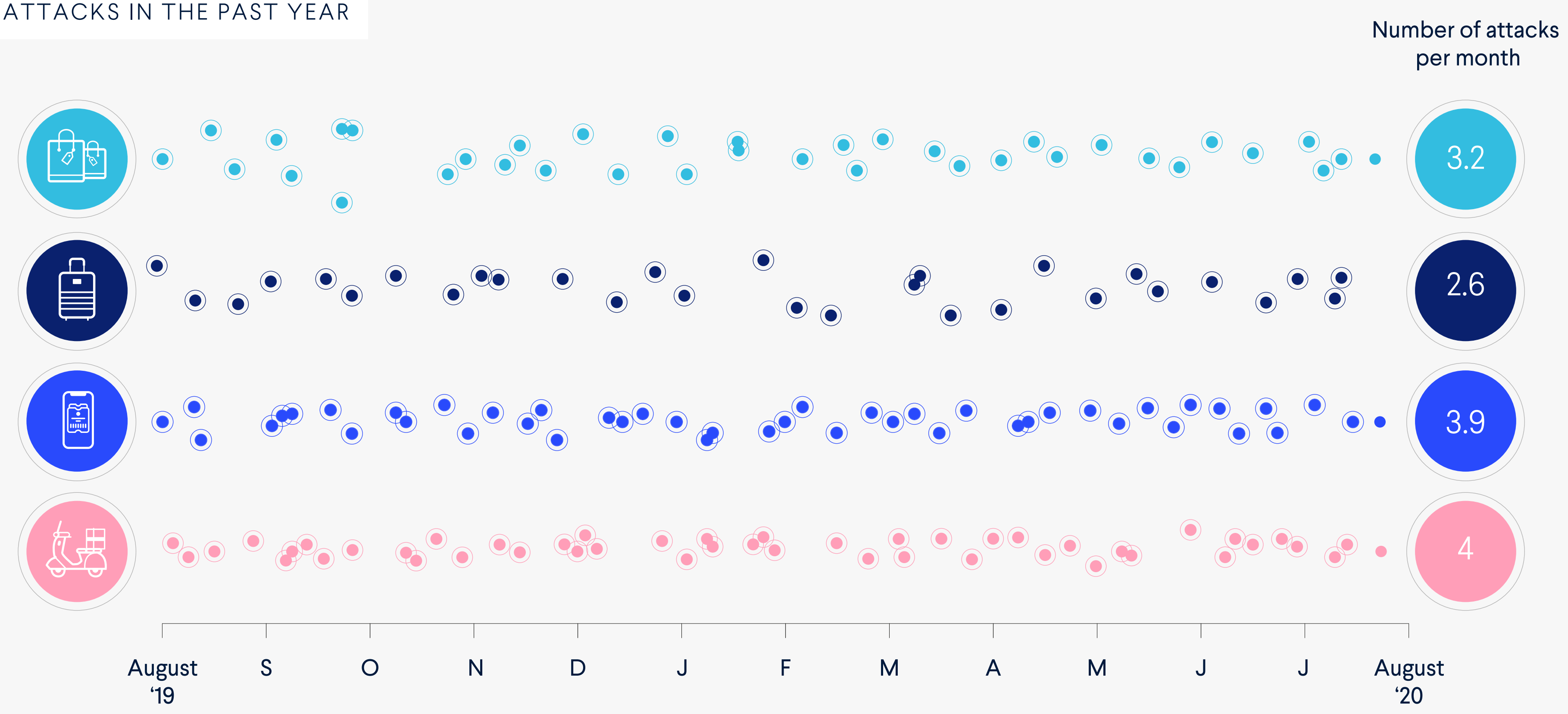
# 9.2 ACCOUNT TAKEOVER

Attacks in the past 12 months

So, we know that not many merchants are tracking the telltale signs of account takeover in customer activities. But how much are they getting targeted by attackers?

We asked merchants roughly how many serious account takeover attacks their business had been the victim of in the past year. These attacks must have impacted a significant number of customers and had a significant, wide-ranging impact.

## ATO ATTACKS IN THE PAST YEAR



The immediate sale nature of Digital Goods and Marketplaces could be a factor behind these industries reporting a much higher number of attacks.

Within the Digital Goods sector, online gambling merchants had very high levels of attacks - an average of 60 in a year. Gambling customer accounts can have significant funds stored in the account which could be very tempting for an attacker.

Also within Digital Goods, Taxi/Cab firms also have a high number of attacks - 65 on average. Like Digital goods, Taxi/Cabs are instant purchases and they have the added benefit for attackers that it doesn't look risky having new addresses and doesn't have to be linked to a specific delivery address. Once the credentials are confirmed, accounts on Taxi/Cab firms can be resold online for a profit for anyone wanting to take a cheap cab ride.

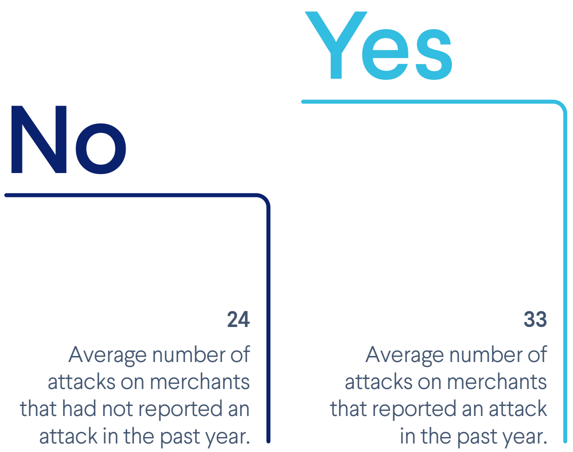
Although the Retail industry has the lowest number of average attacks, within this group Groceries retailers have the highest average - 53 on average over the year. This could have been impacted by Covid-19. At the height of the **peak in the UK**, many online grocery merchants had to restrict orders to existing customers and even limit individual customer orders and specific items for several weeks.

# 9.3 ACCOUNT TAKEOVER

## Reporting high-impact attacks

Overall, all merchants had been aware of at least one account takeover attack on their business, and only 12% of merchants said they were aware of fewer than five attacks in the past year. However, only two-thirds (67%) said that they reported account takeover attacks to the relevant authorities on data privacy. The average number of attacks on merchants that did not report the attacks was 24 – which is a significant number of attacks going unreported.

ATO ATTACKS AND REPORTING

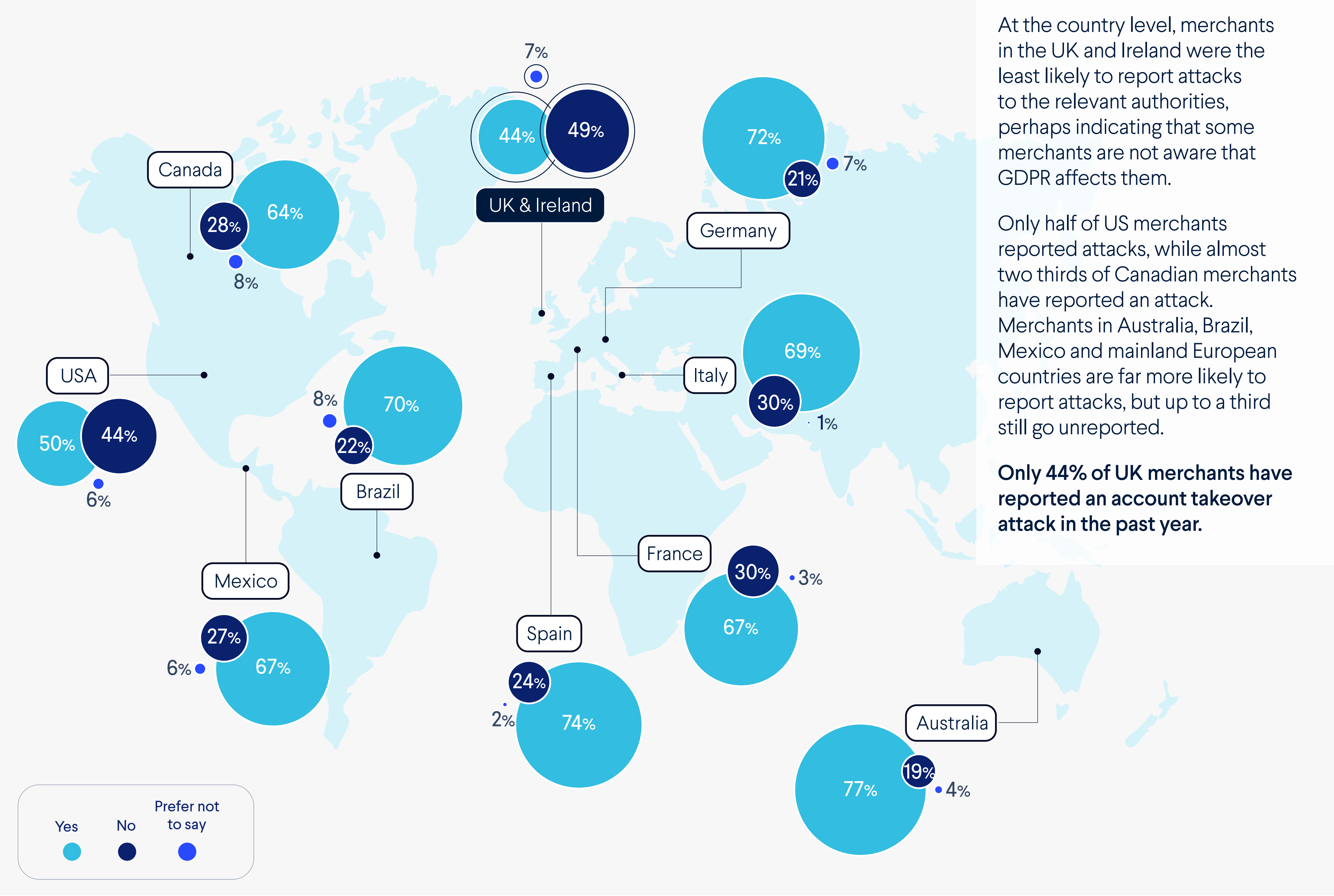


24
Average number of attacks on merchants that had not reported an attack in the past year.

33
Average number of attacks on merchants that reported an attack in the past year.

Why does this matter with regards to ATO? Merchants may believe that if they are a victim of an ATO attack but the original data breach didn't occur on their platform, they are not under any obligation to report it. But this is not the case for merchants operating in Europe under the General Data Protection Regulation (GDPR). **GDPR expands the definition of 'data breach' to include the loss of all data.** Furthermore, GDPR Recital 64 makes it clear that an identity breach (eg. through a successful ATO attack), even of a single customer, counts as a data breach. Therefore, mass ATO logins must be reported to the relevant authorities, and merchants are liable for fines associated with these.

## REPORTING ATO ATTACKS



At the country level, merchants in the UK and Ireland were the least likely to report attacks to the relevant authorities, perhaps indicating that some merchants are not aware that GDPR affects them.

Only half of US merchants reported attacks, while almost two thirds of Canadian merchants have reported an attack. Merchants in Australia, Brazil, Mexico and mainland European countries are far more likely to report attacks, but up to a third still go unreported.

**Only 44% of UK merchants have reported an account takeover attack in the past year.**

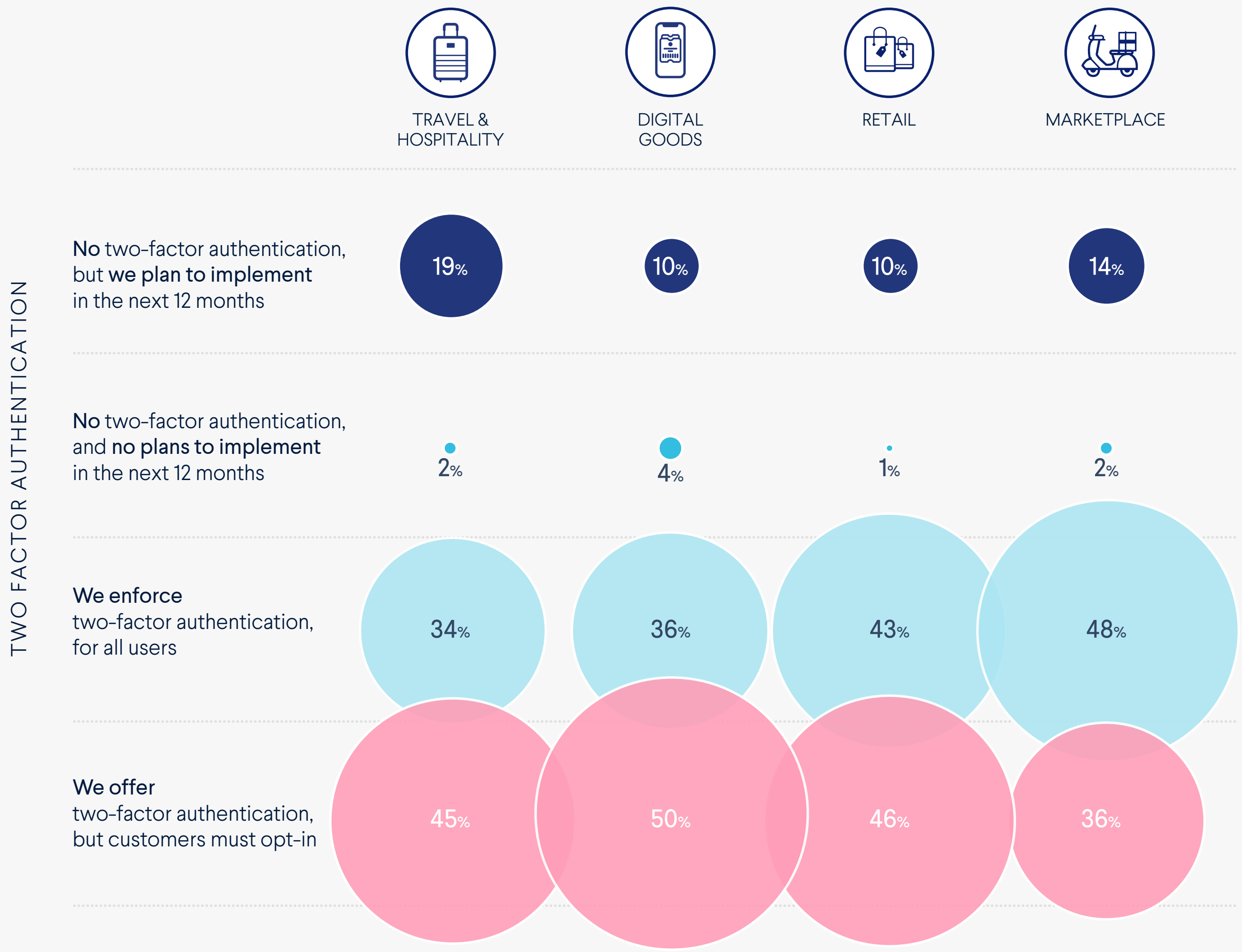
# 9.4 ACCOUNT TAKEOVER

## Two-factor authentication

One of the most effective means for preventing account takeover is two-factor authentication at customer login (2FA). Although 2FA adoption has been increasing, it's still challenging for ecommerce. Many merchants like to offer customers the ability for guest checkout, which means that even registered customers could avoid the hassle of logging into their account.

Despite this, at least a third of merchants in every industry enforce 2FA for all customers. Marketplace merchants, with the highest number of average attacks, are most likely to enforce 2FA. One in five Travel & Hospitality merchants don't offer 2FA. This is not surprising, as travel purchases can be very sporadic and accounts/reorders from customers are not as frequent. . Customers are far less likely to be as loyal to an airline or hotel as they would be to their supermarket.

## MERCHANTS IMPLEMENTATION OF 2FA



When merchants have 2FA, the most commonly offered method is in-app authentication (53%) followed by one-time password (51%), human verification (36%) and finally security questions (24%). Security questions and answers are often available to buy alongside breached credentials, so it's positive that this is not the default choice for 2FA.

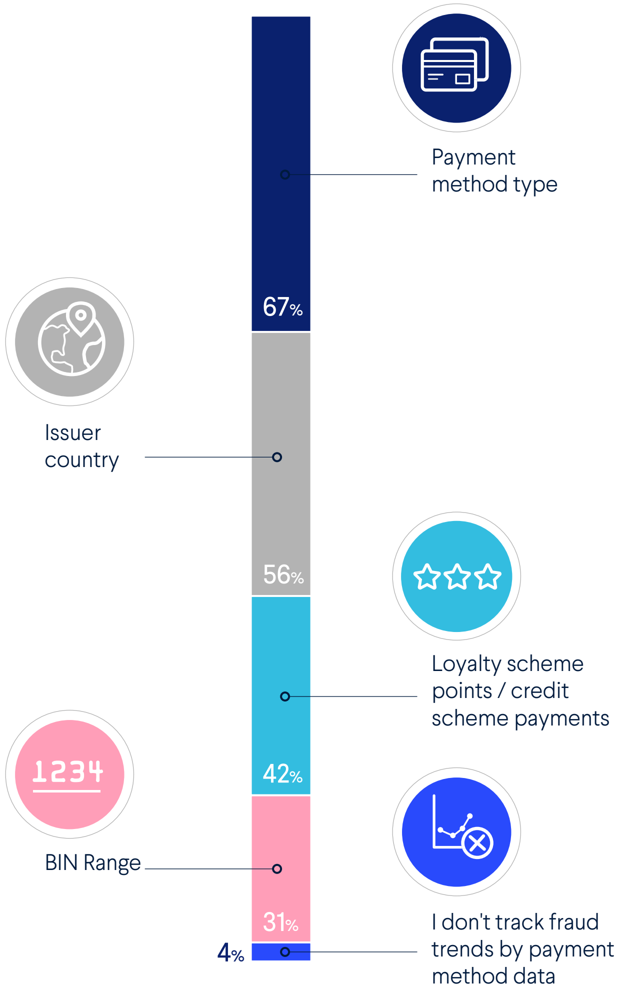
# 10.0 PAYMENTS

## Tracking fraud by payment method

Global payment regulations such as PSD2 in Europe are linking fraud and payments even more closely together, and as we saw earlier, almost 70% of fraud teams also manage payments within their business. It's important to understand whether fraudsters tend to favour specific methods and how they adapt techniques for different payment options.

- Despite this, less than 70% of merchants are tracking fraud by payment method. Knowing more about which methods fraudsters favour would boost merchants' fraud detection ability and enable more sophisticated ways to catch fraudsters out while minimizing friction for genuine customers.

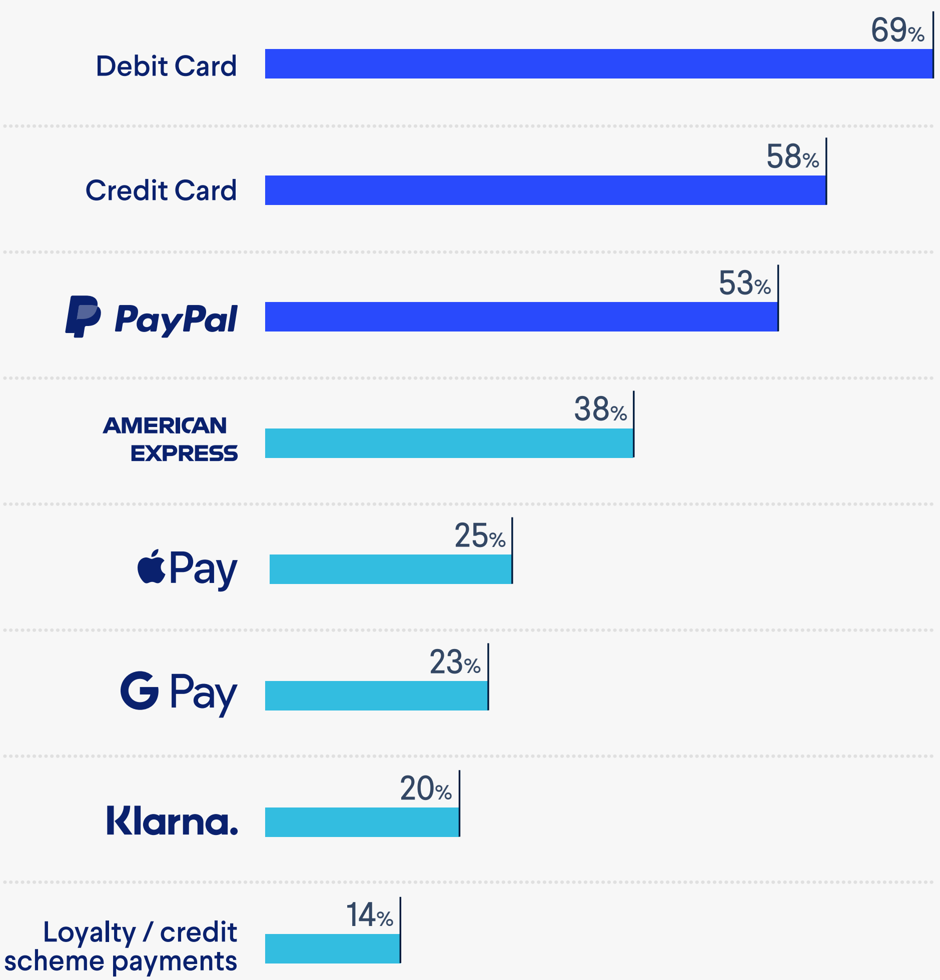
MERCHANTS WHO TRACK FRAUD
**BY PAYMENT DATA**



We asked participants about the top three payment methods they saw the most fraud in. Debit cards were a top choice for almost 70% of merchants, with non-American Express credit cards and PayPal also top for over half of merchants. American Express credit cards were only in the top three for 38%.

ApplePay and GooglePay are a top fraud method for around a quarter of merchants, even though these methods are often portrayed as low-fraud due to the inherent biometric authentication on most phones. But we can see this is not always a guarantee of security, and there is still a risk of fraud. While the phone is biometrically locked to a single user, that user can still add any credit card details they choose. Ravelin conducted a series of independent checks of adding n ew cards to ApplePay and GooglePay wallets, and found that only some banks will verify new cards individually.

**TOP THREE PAYMENT METHODS** FOR FRAUD



# 10.1 PAYMENTS

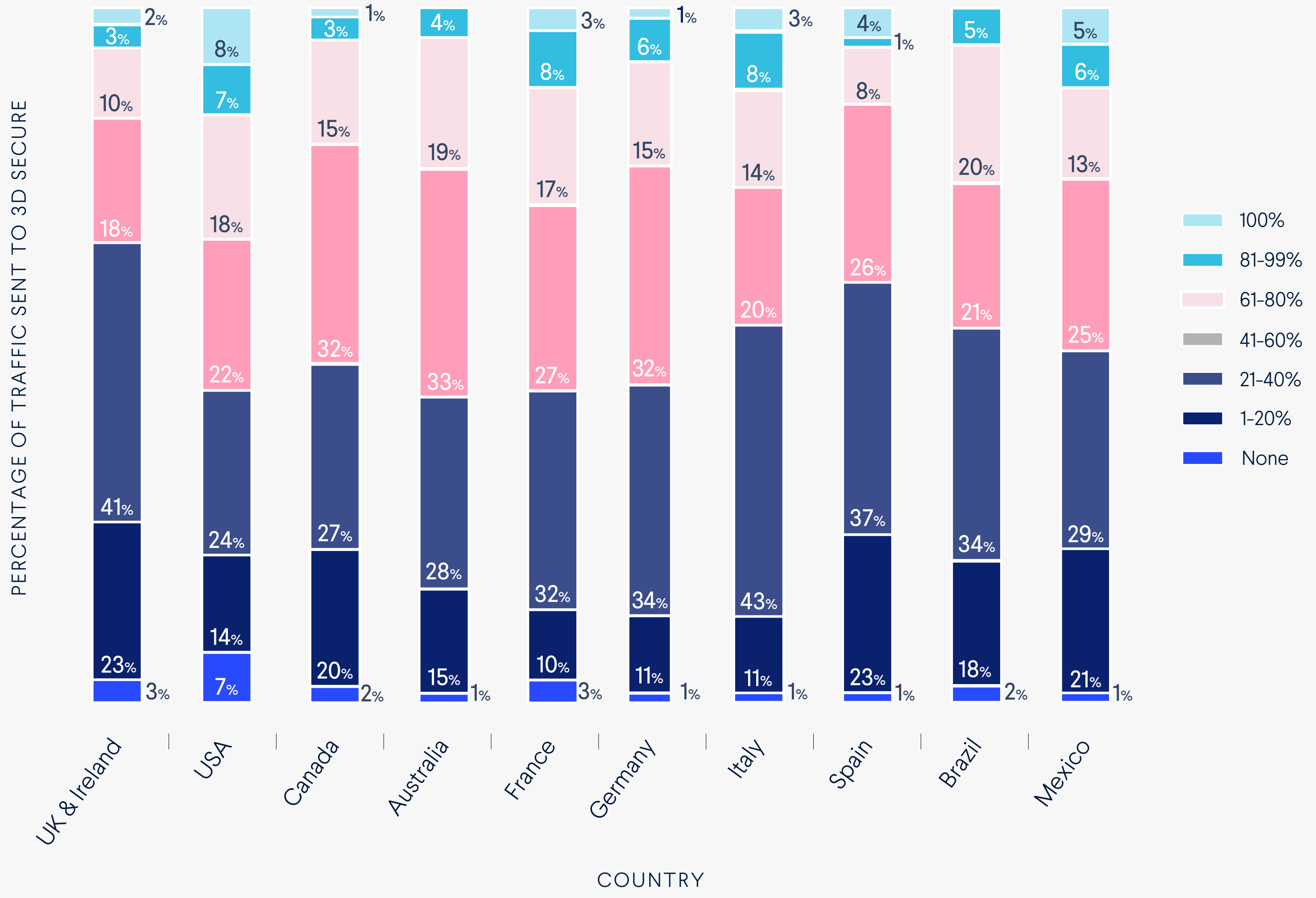
## 3D Secure

3D Secure is becoming more and more widely adopted, and most merchants are sending between 20-60% of their traffic through 3D Secure.

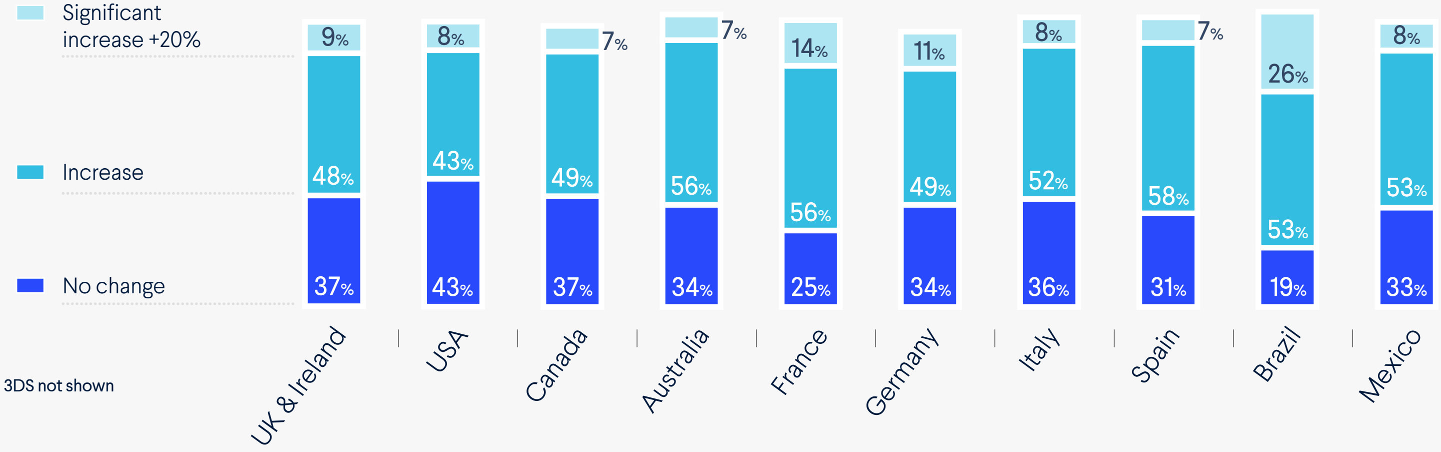
There are some regional variations on the amount of traffic merchants are sending to 3D Secure. Although there are no national regulations requiring authentication in the US at the time of writing, 8% of US merchants are applying 3D Secure on all their transactions – a larger proportion than in any other country and well above the average.

The amount of traffic merchants have sent to 3DS has undoubtedly been impacted by the **regulations coming into force** at the time of the survey (August 2020). Despite the delays to full implementation, by August 2020 Europe's PSD2 has been gaining momentum for over a year. And in Australia, AusPayNet released the CNP Fraud Mitigation Framework on 1st July 2019, requiring Strong Customer Authentication on payments when a merchant's fraud rate is above the limit for two quarters.

## PERCENTAGE OF TRAFFIC SENT **TO 3D SECURE**



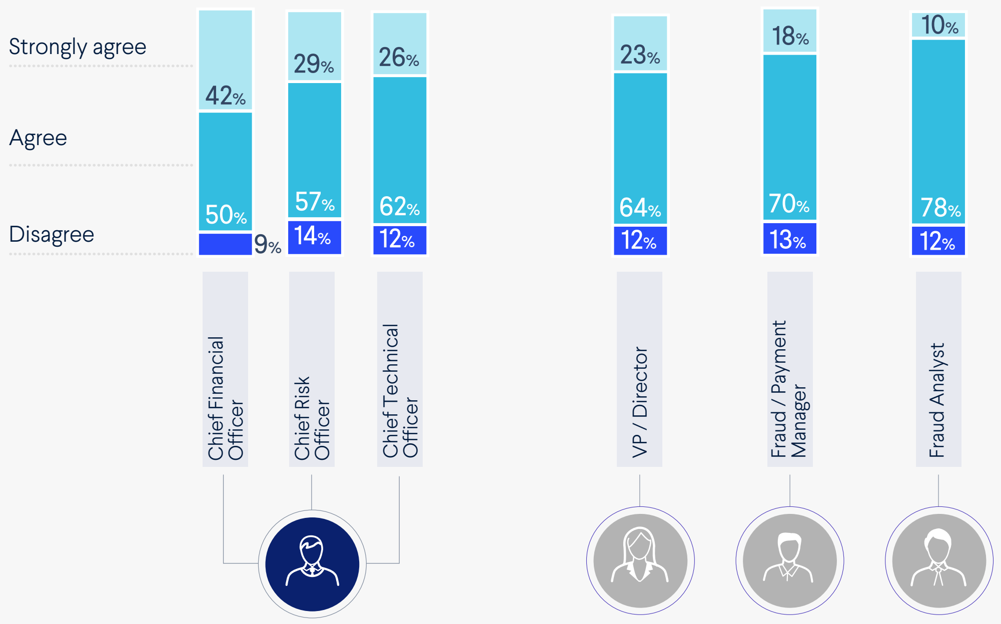
## CHANGE IN NUMBER OF 3D SECURE TRANSACTIONS **IN THE PAST 12 MONTHS***



*decrease in traffic sent to 3DS not shown

We asked participants whether they think that wider use of 3D Secure could reduce the need for fraud tools in the future. Overall, the majority of merchants agree this will happen, with senior level professionals agreeing even more strongly. However, this group was also most likely to predict an increase in fraud budgets and team size in the next year, which could indicate that any predicted reduction in fraud tools is quite a long way off.

## WIDER USE OF 3D SECURE WILL **REDUCE THE NEED FOR FRAUD TOOLS**



# 11.0 EUROPE'S PSD2 REGULATION

## Merchant perception of PSD2

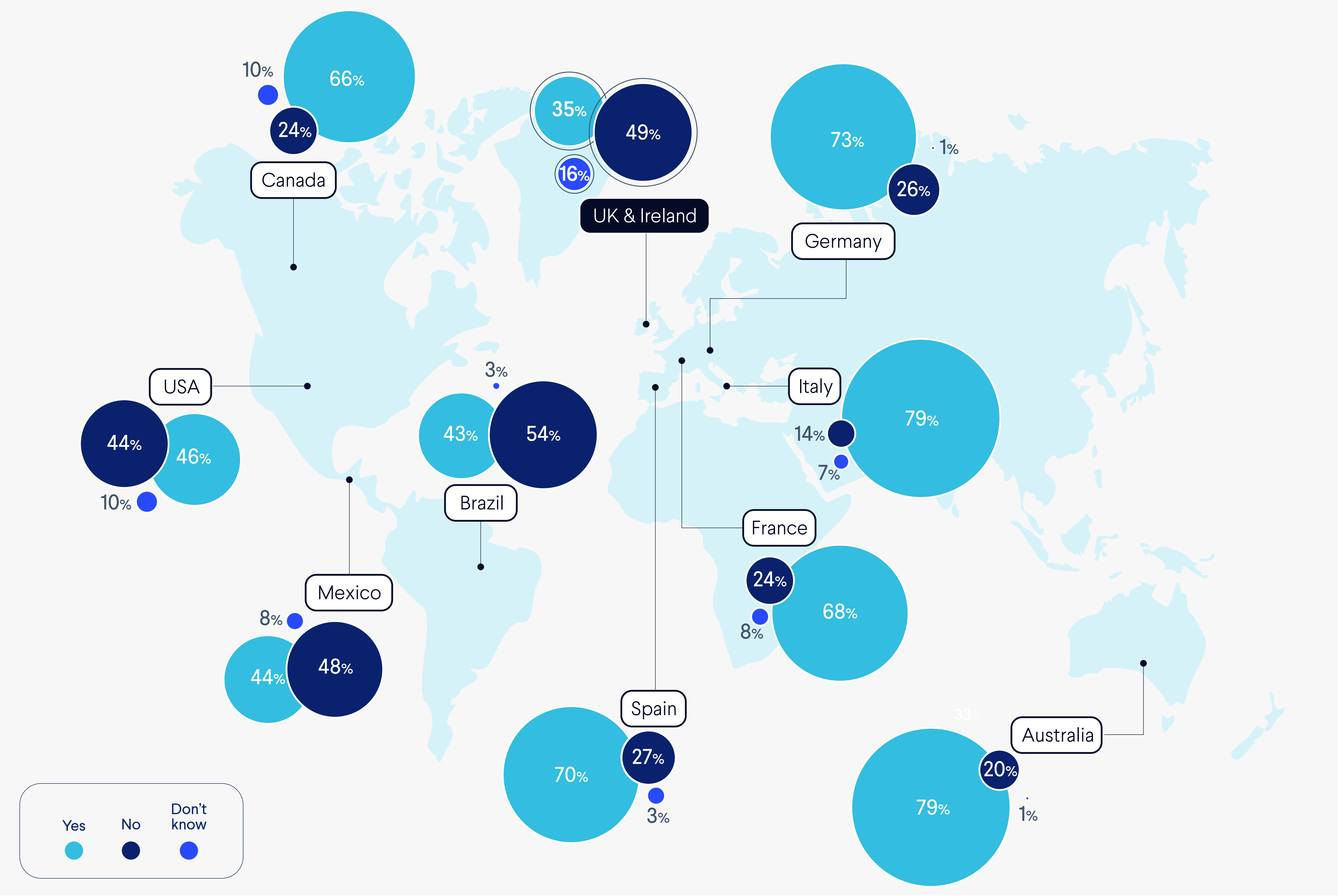
Due to the size of the EU and the global nature of many ecommerce businesses, Europe's PSD2 has implications for online merchants worldwide. Generally, most merchants are aware of this regulation and understand that it will affect them, even if they are not based in the EU.

However, it's concerning that only around a third of UK merchants are aware that PSD2 affects them. Worse, almost half wrongly think it will not affect them, and 16% are in the dark. Of those who don't think PSD2 impacts them, almost 70% have not reported any account takeover breaches to the relevant authorities in the past year. Is it possible that Brexit has led to confusion among UK merchants about which European laws will apply in the UK?

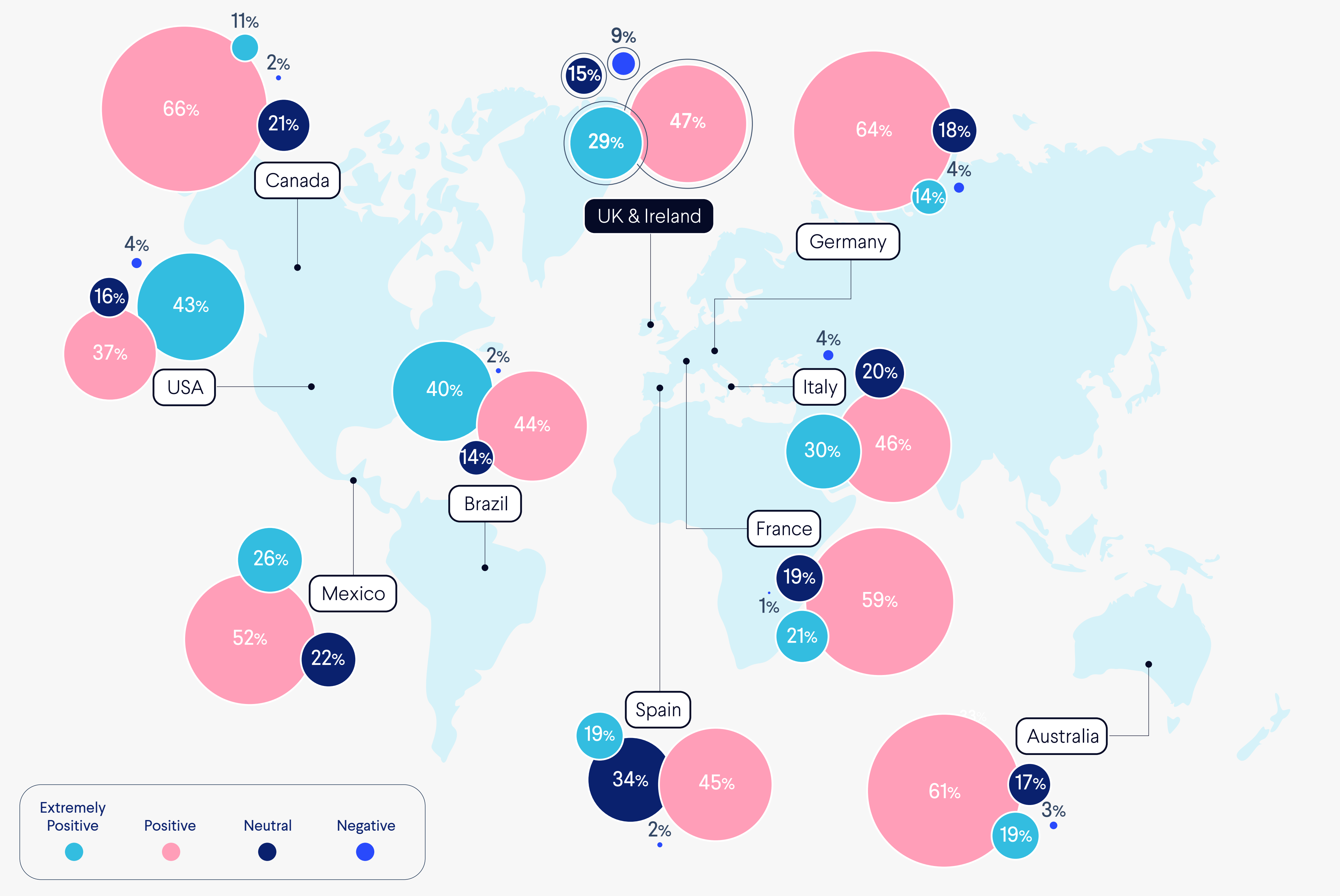
1/3

**Only around a third of UK merchants are aware that PSD2 affects them**

## DOES PSD2 IMPACT YOUR BUSINESS



## PERCEPTION OF PSD2

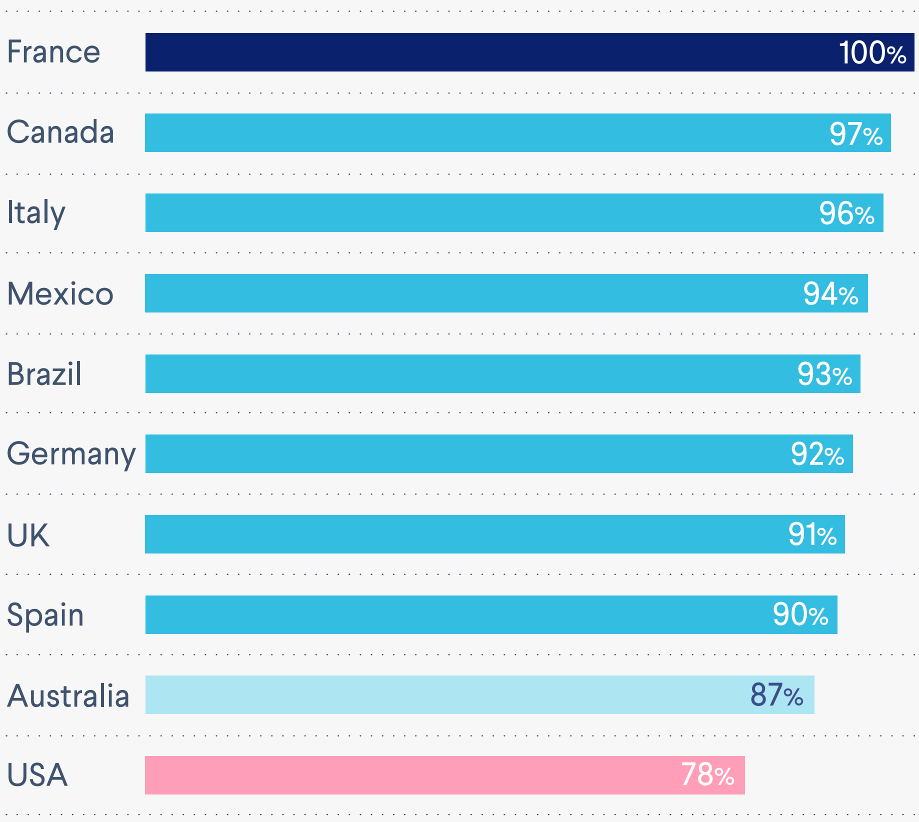


For those merchants that see PSD2 as relevant, the majority see it as having an overall positive impact. This might come as a surprise, as many reports and articles about PSD2 focus on the complexity and the added friction brought by authentication.

43% of US merchants and 40% of Brazil's merchants see PSD2 as having an extremely positive impact on their business. This could mean that they expect to profit from tighter restrictions on Europe's ecommerce sites leading customers to choose smoother buying experiences elsewhere. It could also be that merchants are expecting 3D Secure 2.2 to enable frictionless authentication, as has been promised. However, there's no guarantee that this will happen any time soon and **early results shared by Microsoft do not bode well.**

We asked all merchants who perceived PSD2 as having an impact of them if they expected to be ready for 3DS 2.2 by the European Commission deadline of 31 December 2020. Most of the key European markets expect to be ready, including 100% of French merchants. A surprisingly high number of non-EU markets also expect to be 3DS 2.2 ready, perhaps signalling that merchants have a lot of faith in the upgrade and its promised benefits.

READINESS FOR 3D SECURE 2.2 **BY 31/12/2020**

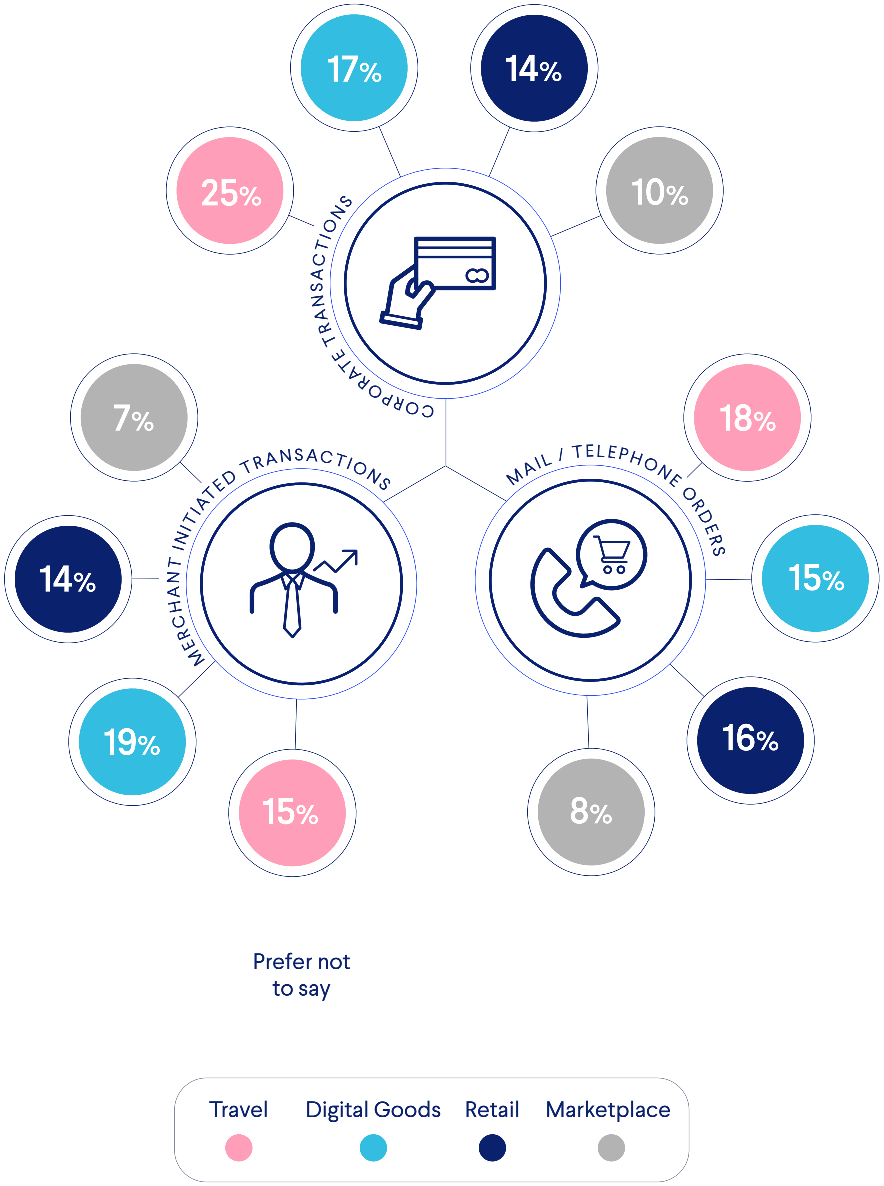


# 11.1 EUROPE'S PSD2 REGULATION

## Out of scope and exemptions

Although PSD2 is largely seen as a positive, merchants expect fraud to increase in fraud in areas which are outside of its scope. A quarter of Travel & Hospitality merchants expect fraud to increase on corporate transactions. This is already a problem area for airlines, as **Tonya Robertson from South African Airlines explained,** corporate referral airline fraud is linked with people trafficking and organized crime.

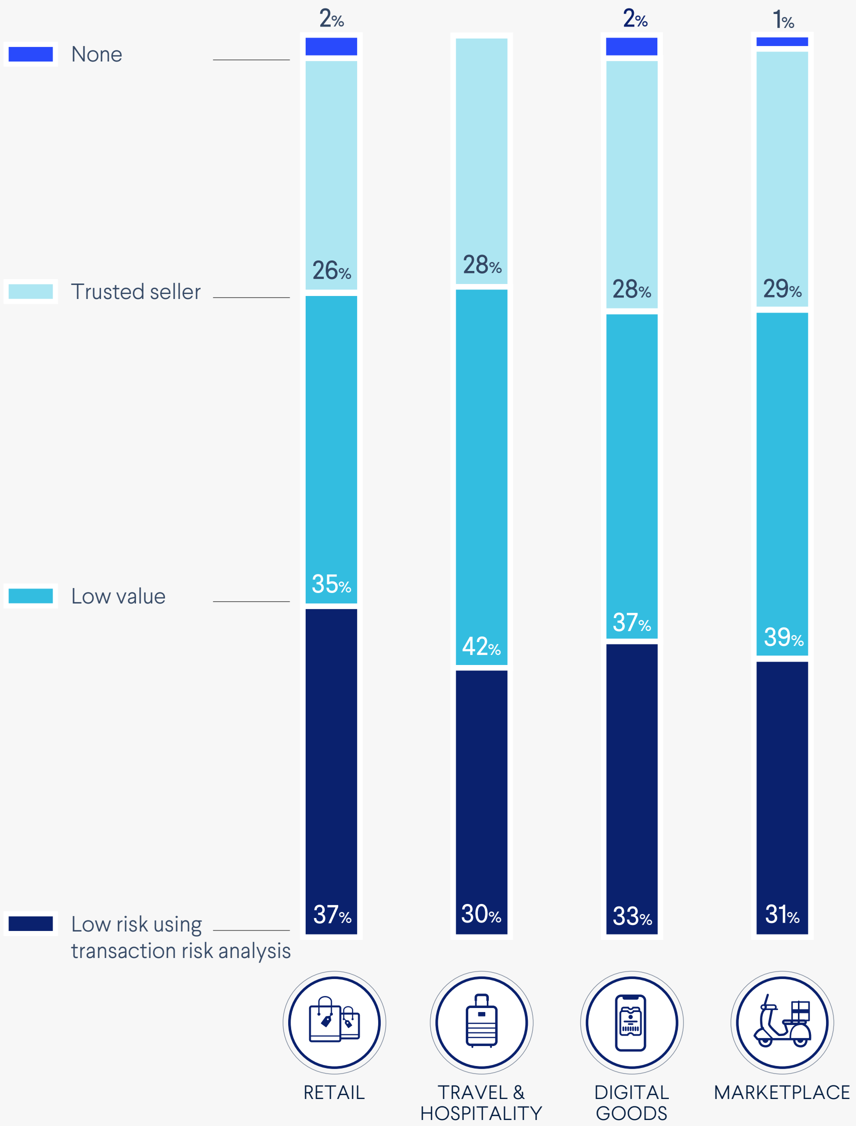
MERCHANTS THAT PREDICT
**FRAUD INCREASE OUTSIDE OF PSD2 SCOPE**



We asked merchants which of the PSD2 exemptions to SCA they planned to use as part of their strategy. Overall, relatively few merchants plan to use each of the exemptions available, in spite of the fact that the majority of merchants expected to be ready to use 3DS 2.2, with the ability for exemptions by 31 December 2020. However, it's important to note that PSD2 was not yet in force at the time of the survey, and the work to prepare for 3DS 2.2 may have been top of mind for many merchants, with the exemptions strategy taking a back seat.

Merchants were most likely to want to use the low value exemption for transactions. Only about a third of merchants plan to use the low-risk exemption to SCA. PSD2 has far-reaching implications for ecommerce merchants and the entire payments ecosystem, and has been widely acknowledged as complex and confusing at times. It may be that many merchants aren't fully aware of the options they have available. To understand more about PSD2 and how the exemptions can benefit merchants, **read our latest guide here.**

## MERCHANTS PLANNED USE OF **EXEMPTIONS**



# 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 FRAUD TEAM DYNAMICS

Most fraud teams have between six and ten people, with over half of Retail, Digital Goods and Marketplaces having teams of 11+. Fraud teams sit in various business departments, there's no single area which works for all businesses.

Experience in fraud is the most desirable factor when it comes to recruiting into the team, ahead of data science expertise and a passion for fighting fraud. Most merchants expect their team and fraud budget to grow, and senior levels are more likely to expect significant growth.

## 2 COVID-19 IMPACT ON FRAUD OPERATIONS HAS BEEN MORE POSITIVE THAN NEGATIVE

Merchant perceptions are mixed, but more merchants say it has been overall positive than negative. Overall, a positive view of Covid-19's impact correlates with an improvement of the wider business perception of the fraud team.

## 3 ONLINE PAYMENT FRAUD IS THE TOP BUSINESS THREAT AND ACCOUNT TAKEOVER, PROMOTION ABUSE AND REFUND ABUSE ARE INCREASING

Online payment fraud is still the number one fraud treat, with account takeover being a close second ahead of friendly fraud. Refund abuse and promotion abuse have increased in over half of merchants, which correlates with changing buying patterns due to Covid-19.

Data breaches and associated fines are merchants' top concerns regarding account takeover. Although most merchants have experienced multiple significant account takeovers in the past year, only two-thirds of merchants have reported these to the relevant authorities.

## 4 INDICATORS OF FRAUD VARY BY INDUSTRY GROUP AND INDIVIDUAL BUSINESS TYPE

Shared industry data is seen as less relevant for identifying fraud. Different industries and business types focus on different factors. It's clear that one fraud detection approach won't work for all merchants and it's important to account for subtle variations.

## 5 FEW MERCHANTS ARE LOOKING AT PAYMENT DATA AND CUSTOMER ACTIVITY TO DETERMINE FRAUD

This is a missed opportunity for merchants to boost their detection accuracy and further their own knowledge of fraudster activity.

## 6 PSD2-AWARE MERCHANTS EXPECT TO BE READY FOR 3D SECURE VERSION 2.2 BY 31/12/2020

However, there's suggestion that many merchants still don't fully understand the implications of PSD2, particularly in the UK. Merchant awareness and understanding of exemptions to SCA under PSD2 also prove there are still some knowledge gaps across all merchants.

# Thank you for reading this 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