Ravelin

GLOBAL FRAUD TRENDS

FRAUD & PAYMENTS SURVEY 2023

ravelin.com

CONTENTS

1.0 INTRODUCTION

It would be fair to say that 2022 was a somewhat paradoxical year for ecommerce. History was made as online retail sales surpassed **$5 trillion** for the first time. And the market saw more businesses "go global" with **76% of shoppers making purchases outside their own countries.**

On the other hand, **customer acquisition costs continued to rise.** And **retail keywords "bulk" and "budget" shot up by around 30%** as customers felt the pinch of inflation. This year also saw the **rise of BNPL options.**

So what has the growing globalized market, a bleak economic backdrop and expanding payment methods meant for fraud and payments? Well, **global losses to ecommerce fraud are set to exceed $48 billion in 2023.** Alongside classic fraud types, newer methods continue to keep fraud teams on their toes.

This report provides insights into:

- Merchant perceptions of fraud and the changing role of the fraud team
- The resources dedicated to fighting fraud both in terms of budget and tools
- Global approaches to authentication and the influence of PSD2

Survey methodology

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

The 2022 survey was carried out using a panel of 1,900 global fraud professionals. Survey participants work for online merchant businesses with over $50 million in annual revenue. The survey was translated into each respondent's local market language for clarity.

Please note that some results may not equal 100% due to rounding.

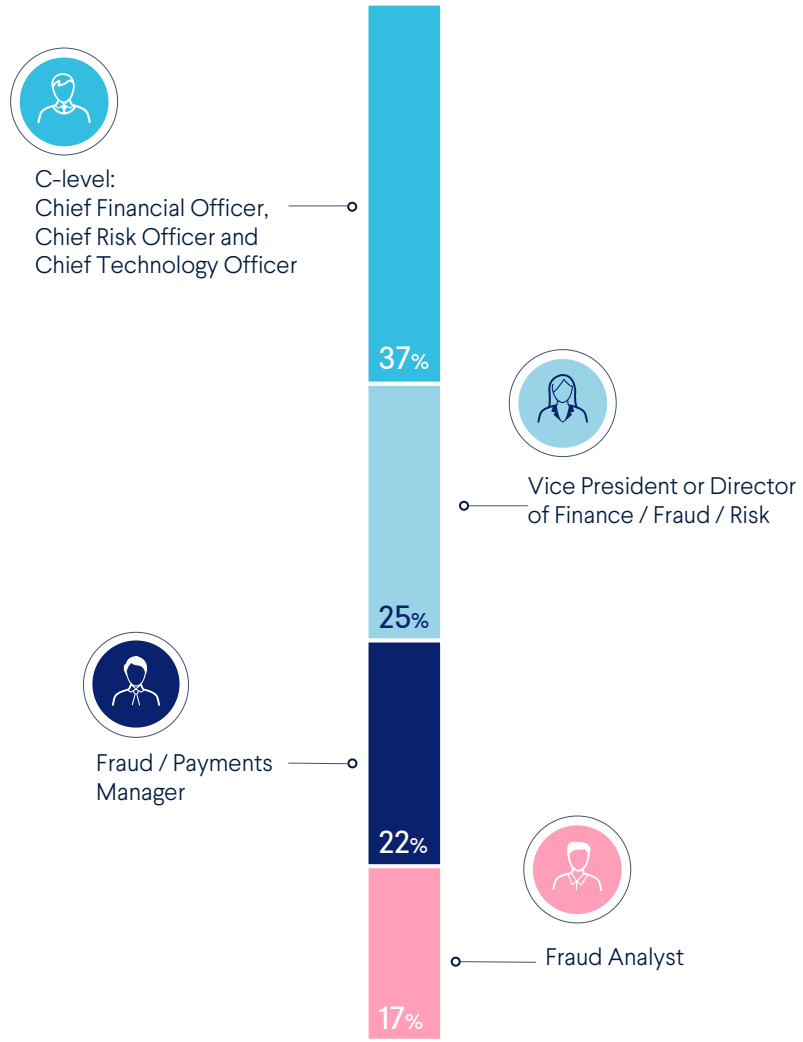
2.0 SURVEY SAMPLE CHARACTERISTICS

Industry, location and job roles

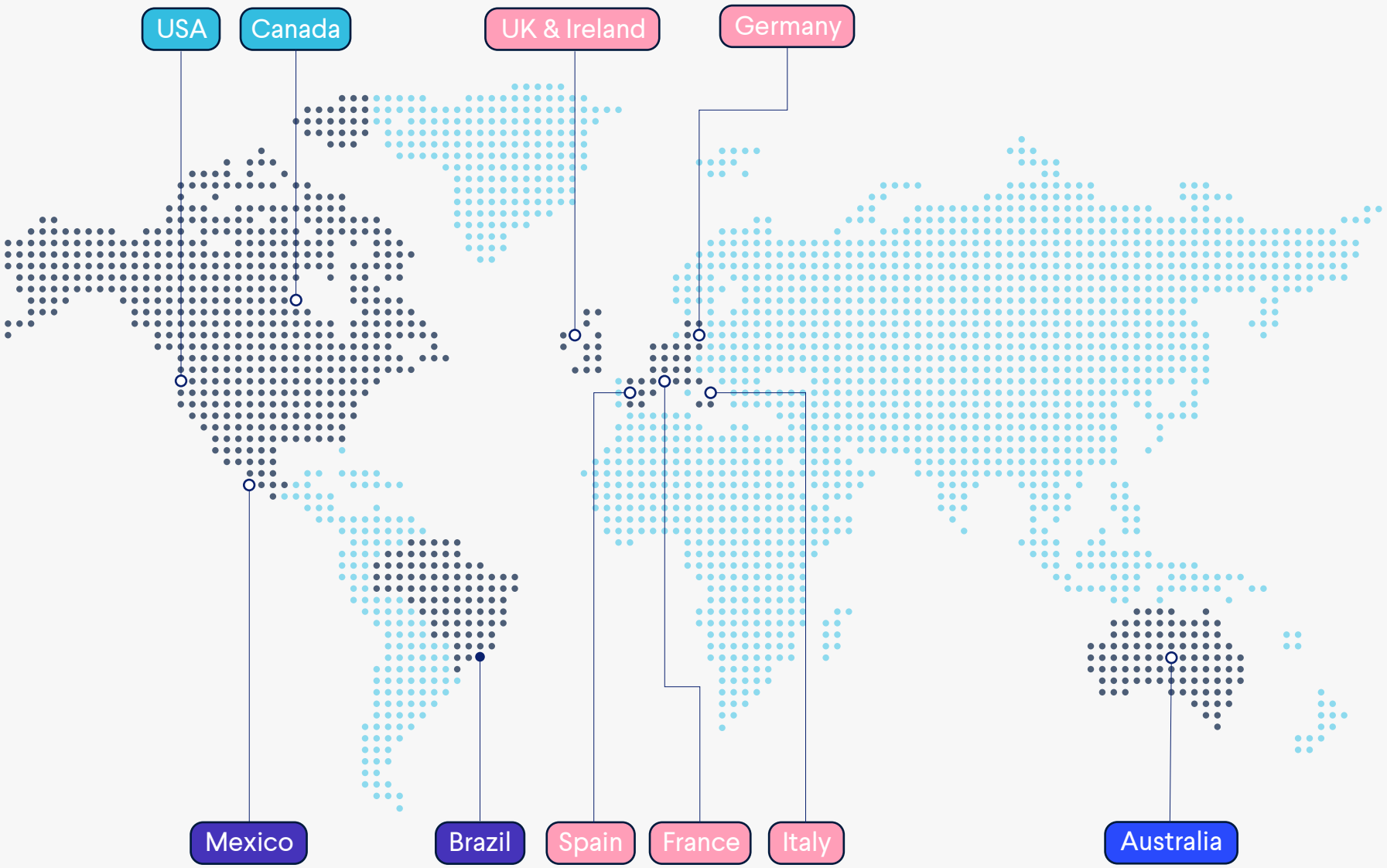
Survey participants are fraud and payments professionals from around the globe. These professionals work in key ecommerce markets in Europe, Australia, North and South America. Survey participants work in a range of business industries under five main groups: Retail, Travel & Hospitality, Digital Goods,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



SURVEY PARTICIPANT **COUNTRIES**



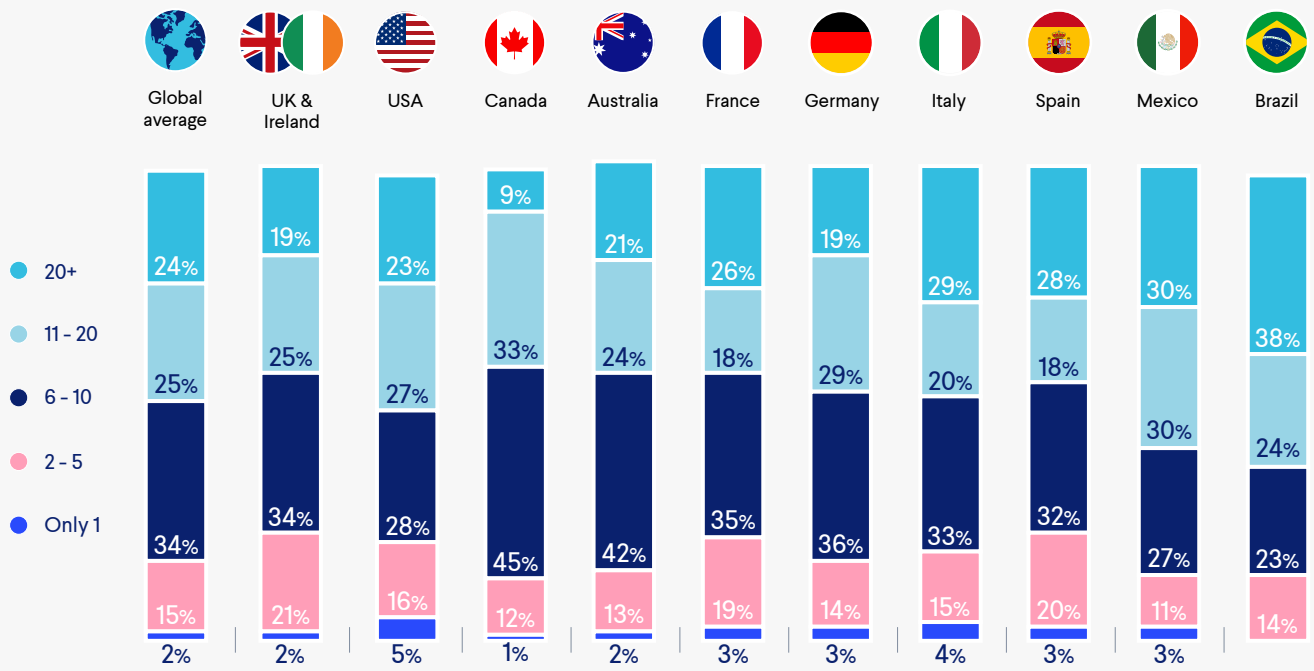
3.0
FRAUD TEAMS

The size, role and perception of the ecommerce fraud team

The fraud team has often been unfairly characterized as an overzealous sales blocker. But this is changing with the rapid growth of the ecommerce market and the fraud that has followed. The truth is strong fraud prevention is a business enabler, but is this how the fraud team is viewed?

HOW BIG IS THE TYPICAL FRAUD TEAM?

HOW MANY PEOPLE ARE THERE IN YOUR FRAUD TEAM?

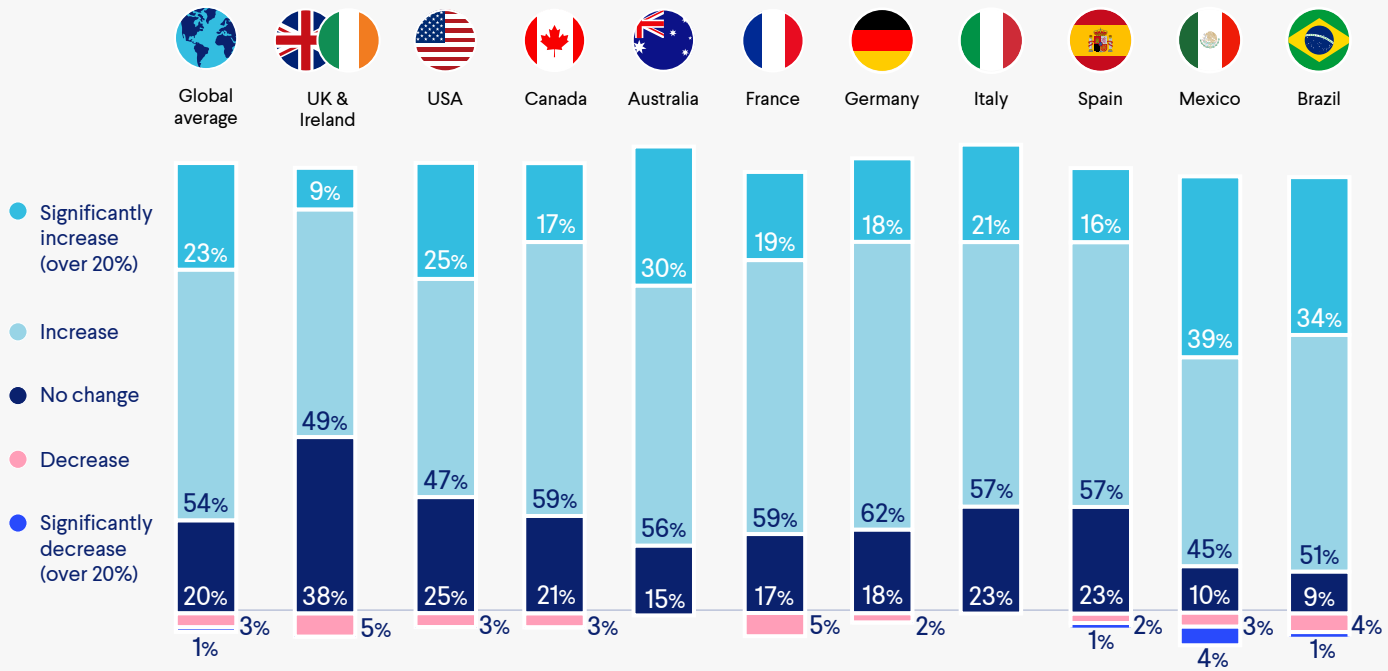


Most respondents report having fraud teams of between six and ten members. And this is what we'd expect to see for businesses of this size. Anything significantly larger or smaller would raise questions about how resources are directed. The aim is to find the sweet spot of a tight but efficient team supported with the right technologies. This is where investing in fraud prevention technology becomes key.

Brazilian fraud teams are notably larger than the global average. Almost 40% say that they have teams of over 20 people. Brazil's ecommerce market is **growing rapidly** and **hiring is often cheaper** in lower cost economies. But the fraud landscape is fast moving, so businesses won't be able to rely on manpower alone for long.

ARE FRAUD TEAMS PREDICTING FURTHER GROWTH IN 2023?

IN THE NEXT 12 MONTHS, HOW DO YOU EXPECT THE SIZE OF YOUR FRAUD TEAM TO CHANGE?

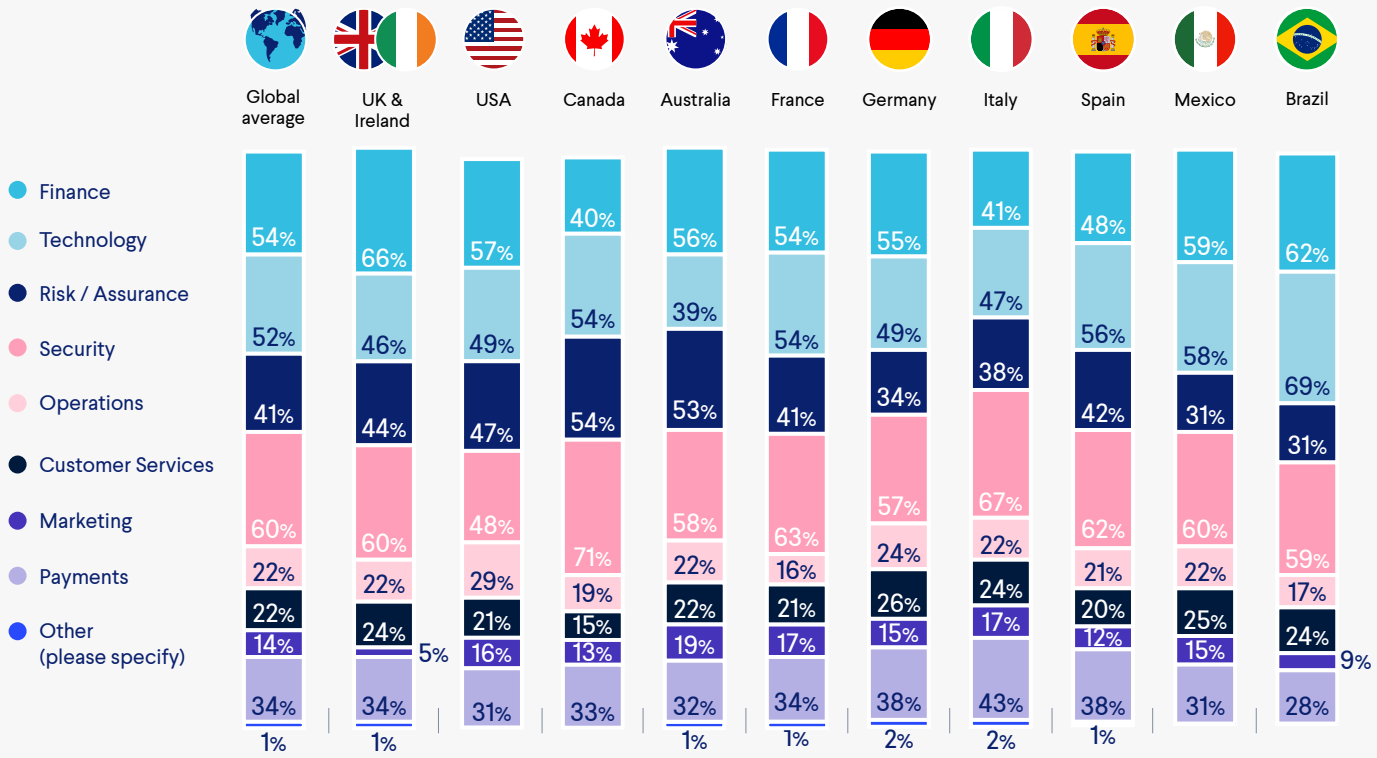


The UK and Ireland are the most conservative with their predictions. Almost 40% of merchants from the region expect no change in fraud team growth – well above the global average. And less than 10% believe that this will significantly increase. This could be down to the tough economic times as the UK faces the worst downturn of any advanced economy.

Australian merchants are way more generous with their forecast for the future. They don't expect any decrease in team size at all and they are the most likely to predict an increase at almost 90%. Mexican and Brazilian merchants reported having the largest fraud teams. So it's interesting to see that around 37% of merchants from this region predict that their teams will grow by over 20%.

WHO ARE YOUR FRAUD TEAM'S CLOSEST COLLABORATORS?

WHICH DEPARTMENTS DOES YOUR FRAUD TEAM WORK MOST CLOSELY WITH?

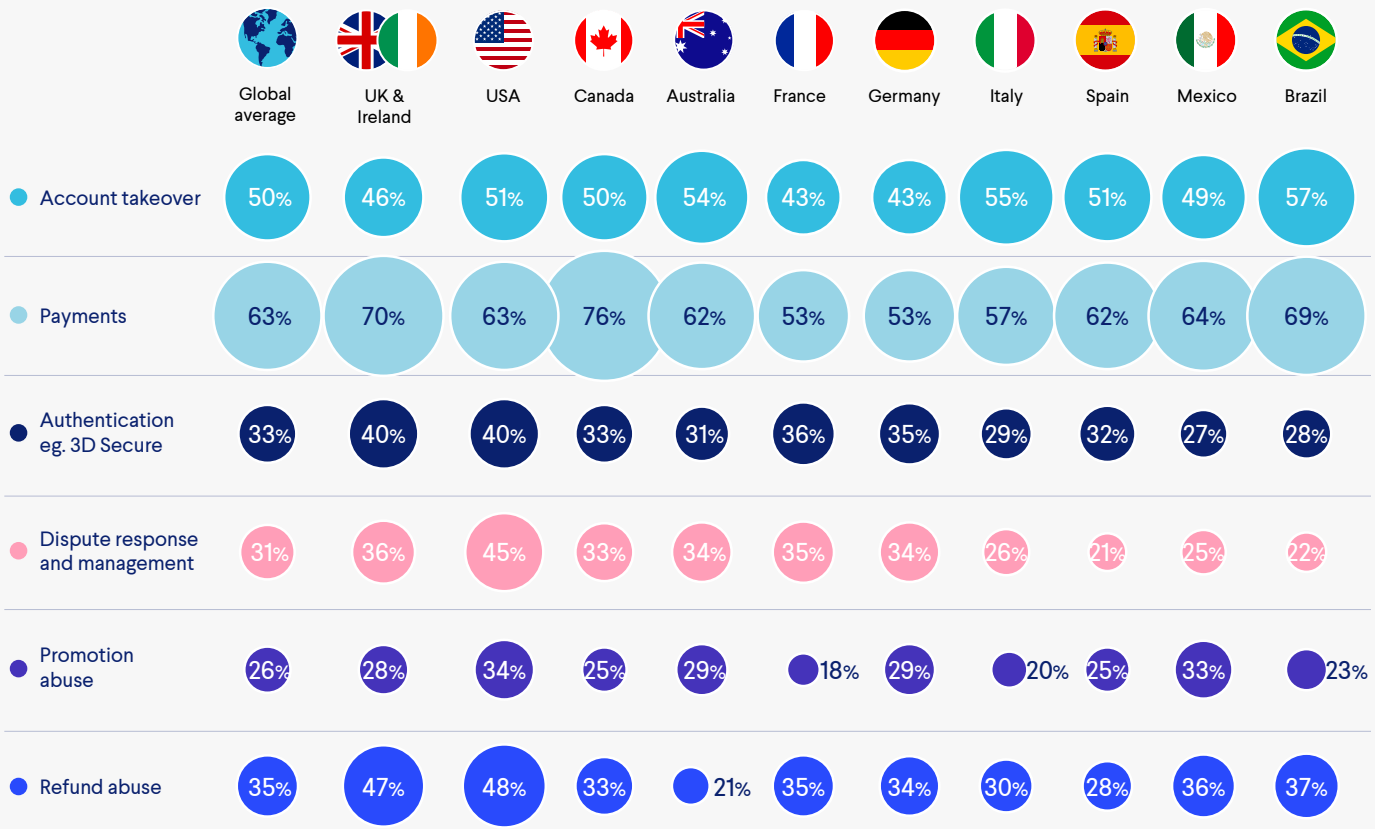


Overall fraud teams globally seem to work most closely with the Security, Finance and Technology teams. Only Italian fraud teams report working closer with the Payments team. But we could see this become the case more broadly with the **growth of the payments market** and global advancement in 3DS protocols.

Only 14% of fraud teams report working closely with the Marketing team. This is exceptionally low when we look at the growing **threat of promotion abuse** to revenue. It's vital that your fraud teams engage with company marketing activities. The same goes for the Operations team when you're trying to tackle costly fraud risks, like fake accounts and **fraudulent refunds/returns.**

WHAT ARE YOUR FRAUD TEAM'S RESPONSIBILITIES?

WHAT RESPONSIBILITIES DO YOUR FRAUD TEAM MANAGE TODAY, OTHER THAN CONSUMER FRAUD MANAGEMENT?

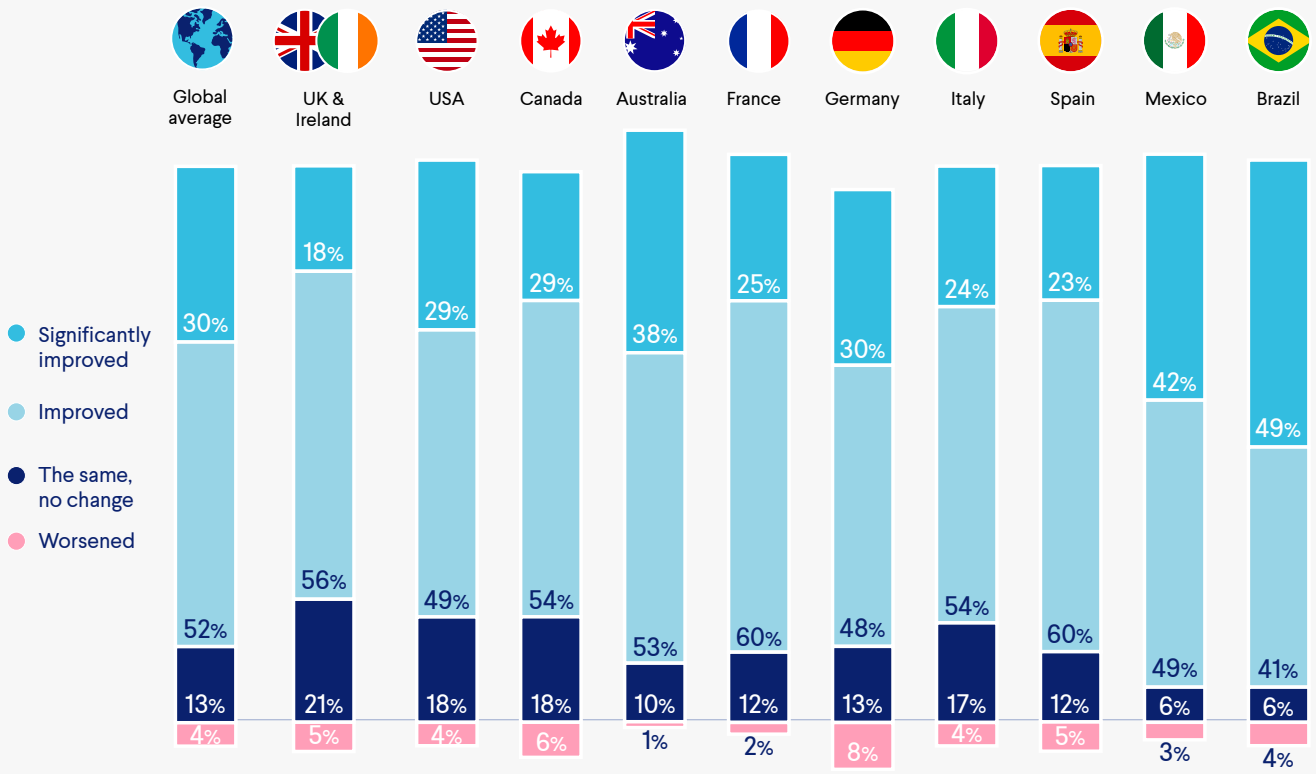


The varying responses go to show that there's no hard rule to what the fraud team's responsibilities are. How you divide your team's labor will likely depend on your business's priorities. That said, more teams seem to be responsible for payments and account takeover, in addition to online payment fraud.

Almost 50% of American, UK and Irish merchants say that they handle refund abuse. This is close to those who are responsible for account takeover. This could be due to a disproportionate growth in returns and refund fraud in those regions. In the US alone, **fraudulent online retail returns amounted to a whopping $23.2 billion in 2021.**

HOW HAS THE PERCEPTION OF THE FRAUD TEAM CHANGED?

HOW HAS THE PERCEPTION OF YOUR FRAUD TEAM WITHIN THE BUSINESS CHANGED IN THE PAST 12 MONTHS?



Perception of the fraud team continues to improve year on year. This is the feedback from respondents across the business, including those at C-level. This is great news! As we'll discuss later, businesses are having to contend with increased fraud exposure. So fraud prevention is integral to any growth or revenue protection plans a business might have.

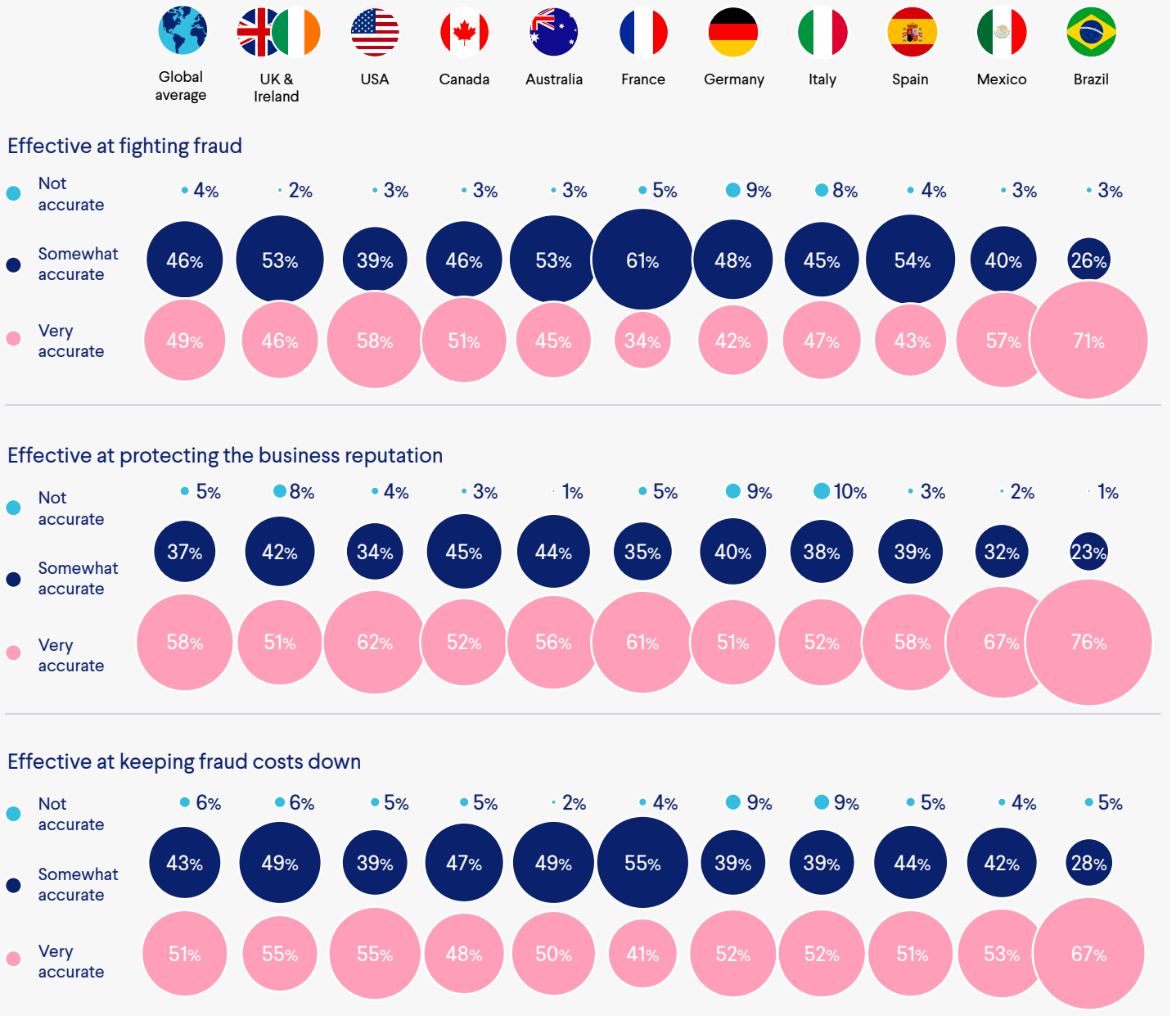
But it's hard to ignore that almost 10% of German respondents say that perception has actually worsened. Could the fraud team be facing blowback from **expanding fraud threats** in the country?

HOW EFFECTIVE IS THE FRAUD TEAM IN THE EYES OF THE WIDER BUSINESS?

We wanted to dig further into how the fraud team is perceived by the wider business. How do your colleagues feel about your ability to fight fraud, protect the business reputation and save money?

Brazilian merchants have the most positive outlook. The percentage of Brazilian merchants who answered "very accurately" to whether they're recognized for their efficacy was above the global average across the board.

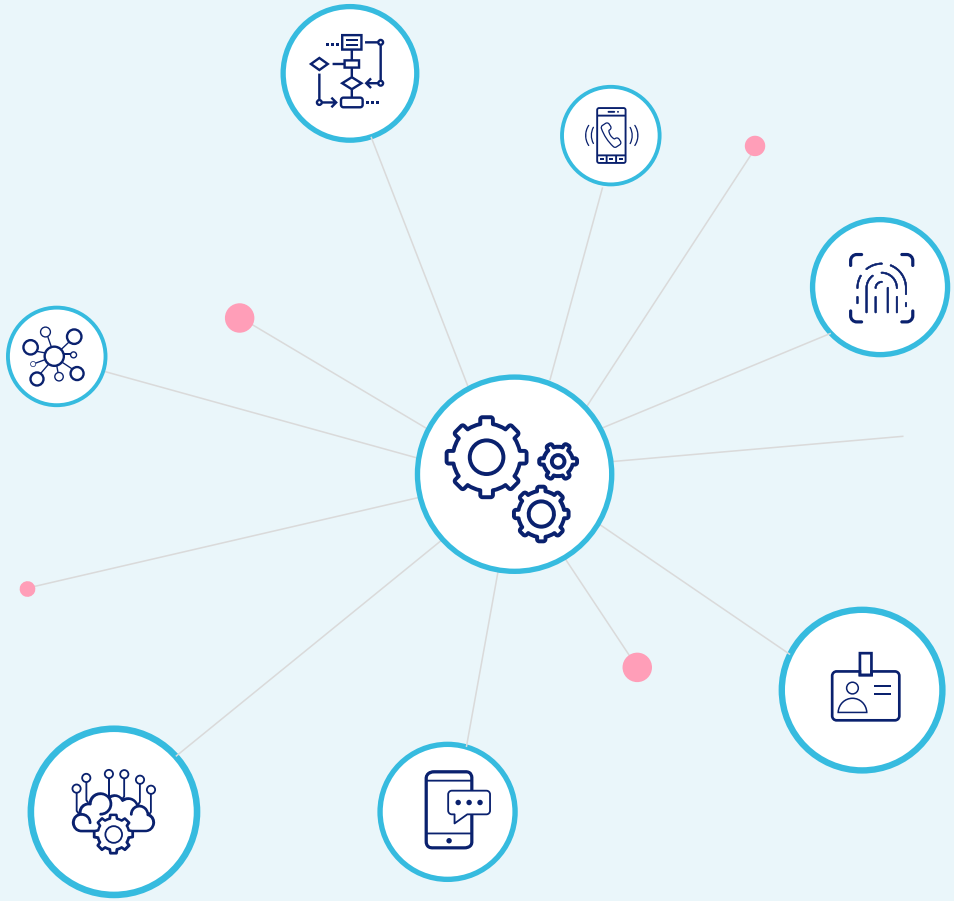
German and Italian merchants have a much more pessimistic take on how they're regarded by the business. Almost 10% don't think they're seen as effective in any of these areas.



4.0
TOOLS & BUDGETS

The adoption, cost and impact of fraud solutions

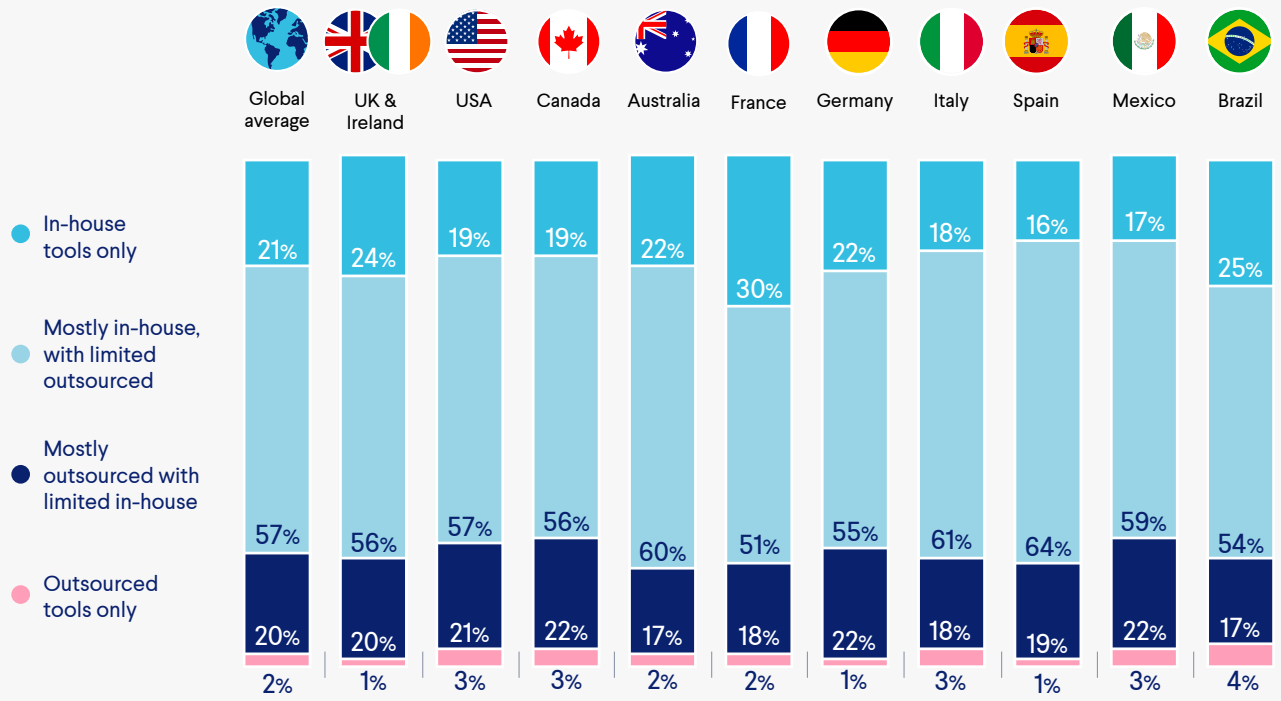
The global fraud detection and prevention market is **expected to exceed $190 billion in 2030**. And this is out of necessity. The expanding ecommerce market is a treasure trove of access and opportunity for scammers. On top of this, yesterday's fraud is not necessarily today's fraud. So you can't afford to get complacent. What's in your arsenal?



ARE MERCHANTS USING IN-HOUSE OR OUT SOURCED TOOLS?

We wanted to find out where merchants are getting their tools from. Are you building your own or have you enlisted the expertise of a third party provider?

TO COMBAT FRAUD, ARE YOU USING IN-HOUSE TOOLS, OUTSOURCED TOOLS, OR A MIX?



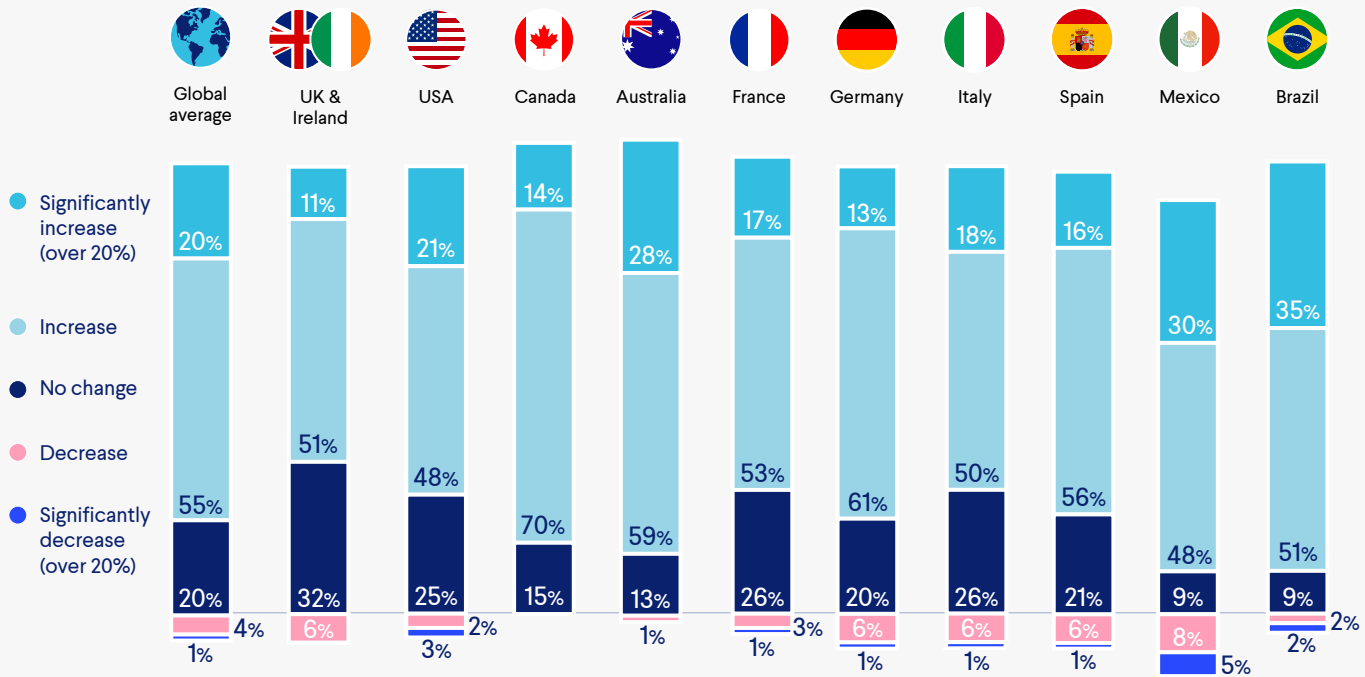
Around 80% of merchants are using outsourced tools to some degree. But this is limited for about 60% of them. Clearly there is some value to maintaining some home-built capabilities. But we can't deny that relying on internal solutions quickly becomes unsustainable as a business grows.

In-house solutions are more expensive to maintain than replace over time. So, you would expect that businesses of this size would use more outsourced tools.

80%
are outsourcing tools

WILL FRAUD BUDGETS GROW IN 2023?

IN THE NEXT 12 MONTHS, DO YOU EXPECT YOUR BUDGET FOR FRAUD PREVENTION TO INCREASE OR DECREASE?



We asked merchants how their budgets for fraud prevention will change in the coming year. The majority of merchants see their budgets increasing. But there are a couple of results that stick out.

Around 40% of Mexican merchants predict that their team size will grow by over 20%. So it follows that a third of merchants from this region would also see budgets increasing by over 20%. Strangely though, Mexican merchants are the most likely to say their budgets will drop at 13%.

Canadian merchants are also feeling optimistic on this front – none of them predict a decrease. In fact, a whopping 84% say that budgets for fraud will likely increase.

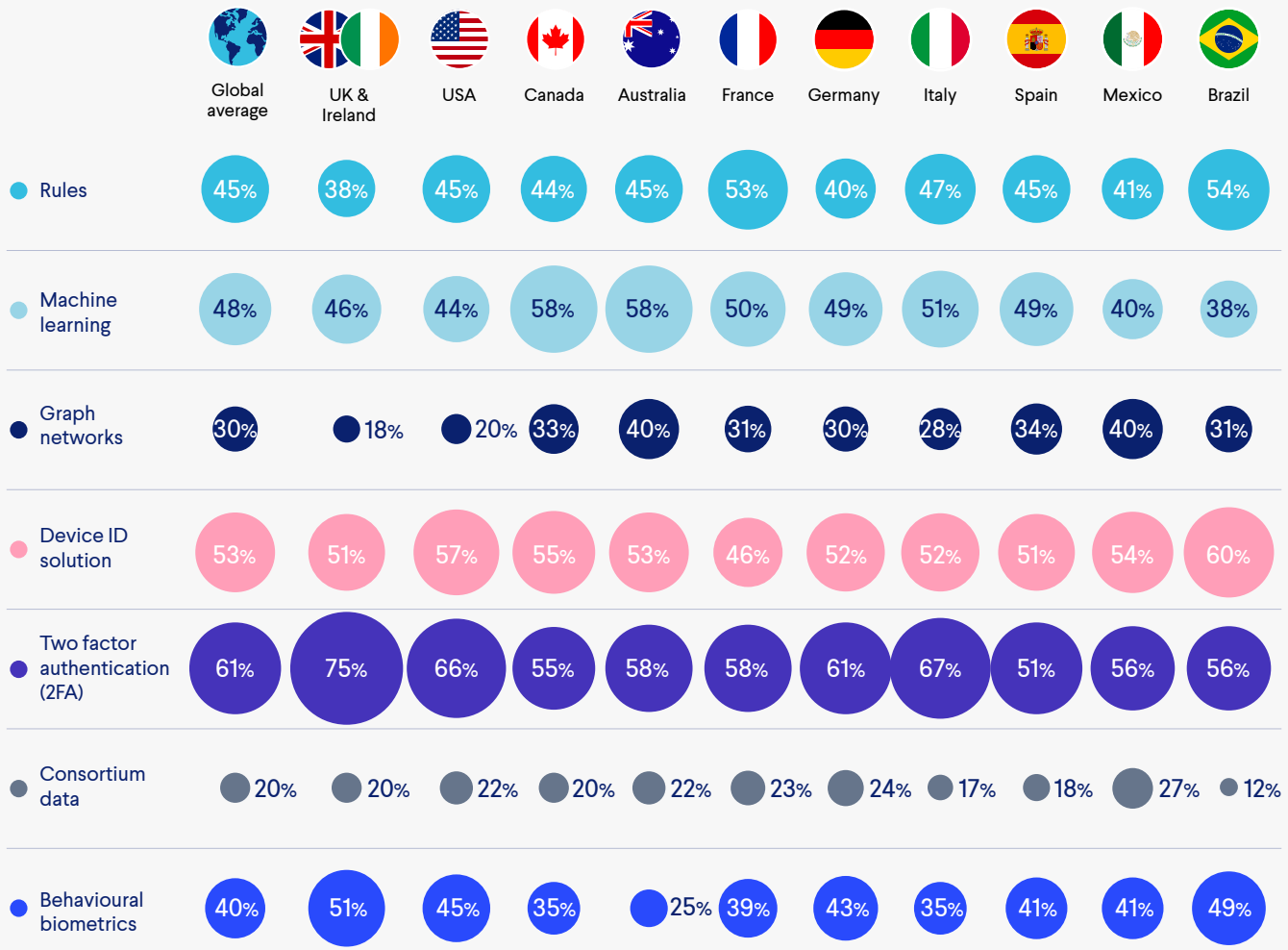
WHAT TOOLS ARE MOST EFFECTIVE IN FIGHTING FRAUD?

Merchants are putting their money where their mouths are, but which techniques are actually getting the job done? Looking at the feedback across regions, there isn't a singular fraud strategy that's most effective.

This supports the argument that you can't take a one and done approach when it comes to fraud. Different solutions are effective at fighting different frauds. And having a robust toolstack allows you to take into account the dynamic nature of fraud.

Your fraud strategy should include most, if not all, of these tools. It's a question of getting the blend right between the various strategies that will deliver a solution that is effective in the long term. This is where partnering with a fraud provider could really change the game for your business.

WHICH OF THE FOLLOWING TOOLS DO YOU FIND MOST EFFECTIVE FOR FIGHTING FRAUD?



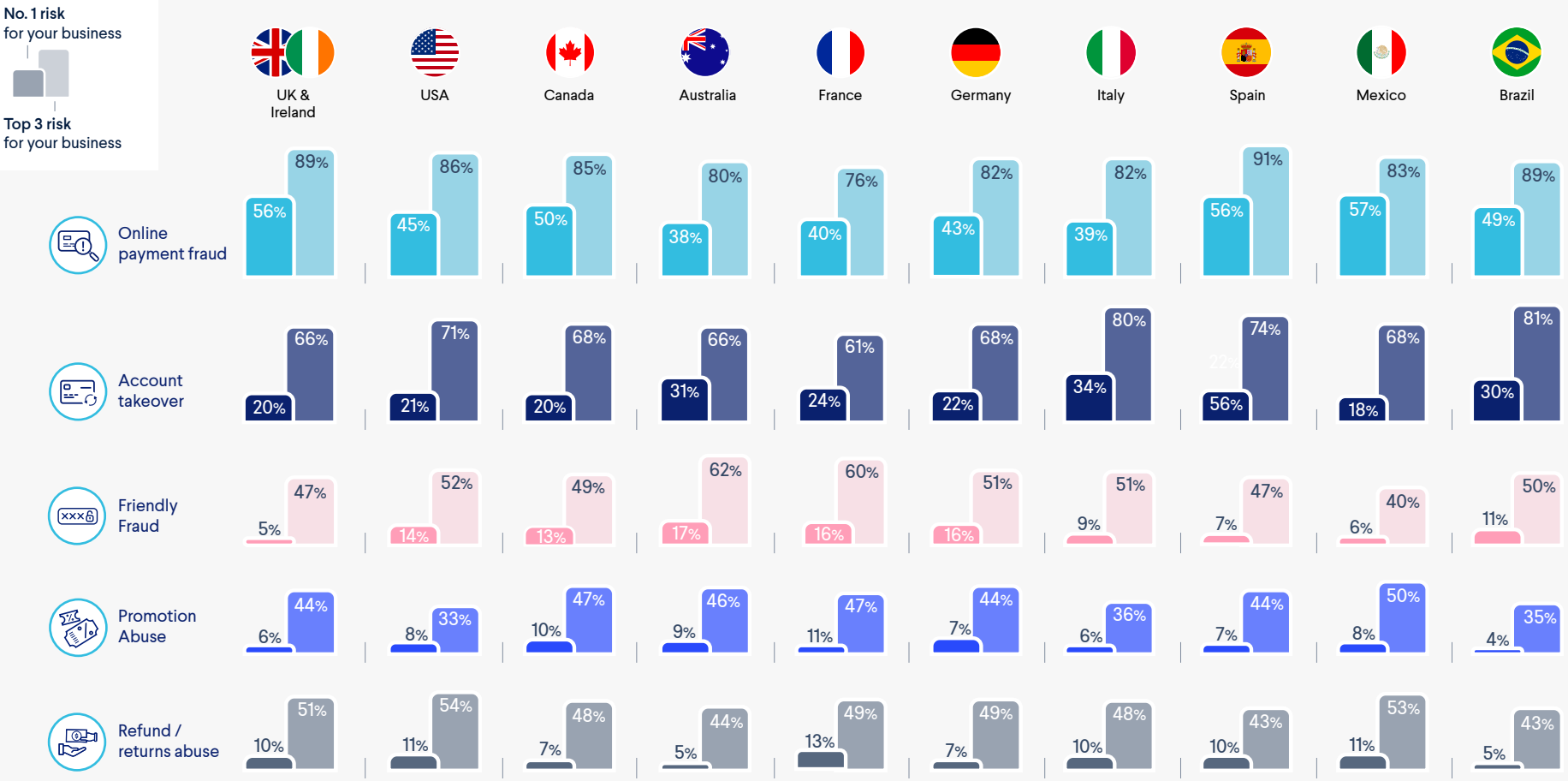
5.0 MONITORING FRAUD

Growing threats: the scale and growth of fraud

Around **25% of sales will be from online purchases in 2025.** This is great news for your business. The downside is that cybercriminals continue to capitalize on this shift.

Fraud is on the up and losses will cost merchants **well over $48 million in 2023.** But where are you most vulnerable? We asked merchants across the globe to rank the biggest threats to their business.

WHAT ARE THE TOP FRAUD RISKS TO YOUR BUSINESS?



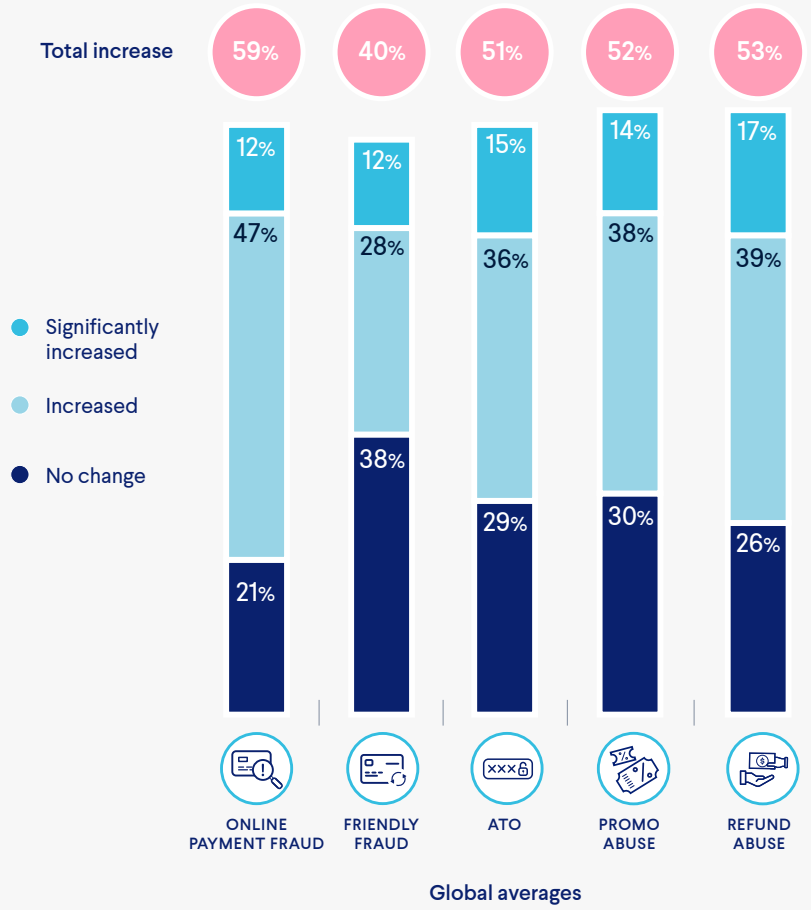
Unsurprisingly, online payment fraud and account takeover remain the top threats across regions. But has 3D Secure (3DS) seen fraudsters vary tactics and driven an increase in the other fraud tactics? You'd expect to see a notable difference in Europe compared to the other regions if so. But so far that hasn't been reported by our respondents.

It also looks like you won't just have to watch out for the professional fraudster. Opportunistic behavior from genuine customers is on the rise as money gets tighter. Could friendly fraud and policy abuse be more of a risk than meets the eye?

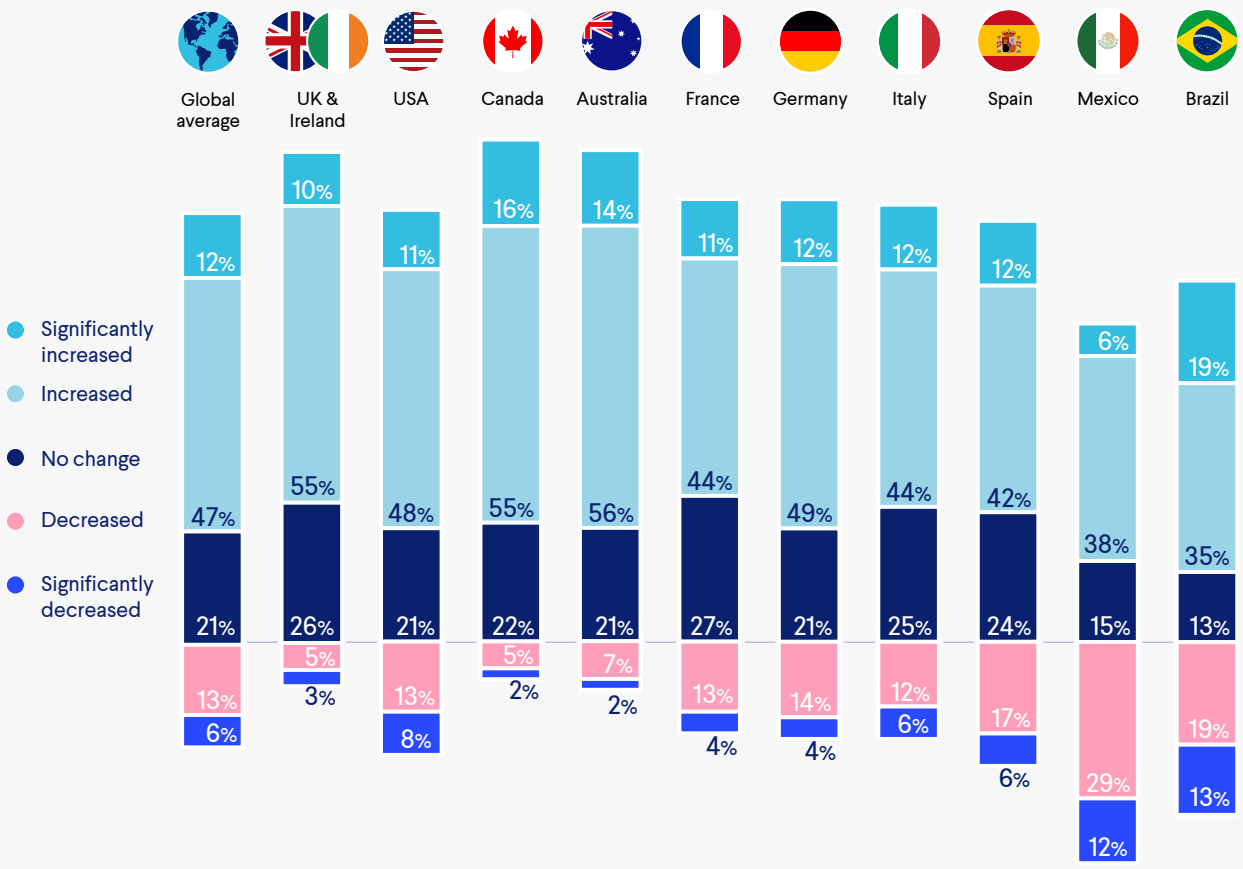
DID FRAUD INCREASE IN 2022?

We know that ecommerce fraud is on the rise, but how do things look from your end? We wanted to find out the merchant perception of fraud levels over the past 12 months.

IN THE PAST 12 MONTHS, HOW HAVE THE LEVELS FOR EACH OF THESE TYPES OF FRAUD CHANGED?



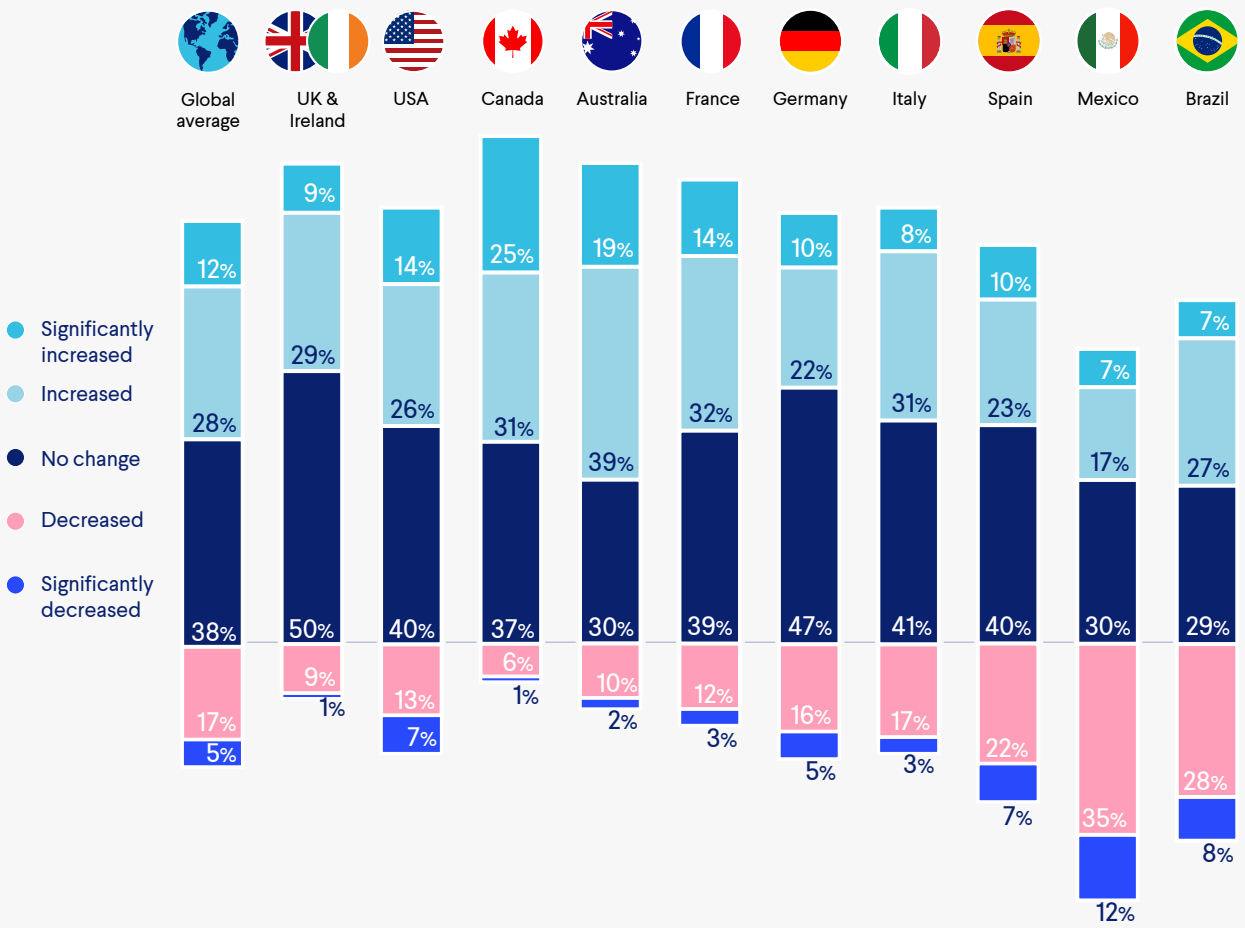
ONLINE PAYMENT FRAUD



Almost 60% of merchants globally say that online payment fraud has increased over the past 12 months – that's up from 56% in 2021. Canadian and Australian merchants are the most likely to report seeing an increase at around 70%.

This result isn't completely unexpected. But there is hope that better authentication practices could slow this down. Secure Customer Authentication is already mandated across Europe. And **we're seeing other nations cautiously follow suit with growing 3D Secure adoption.**

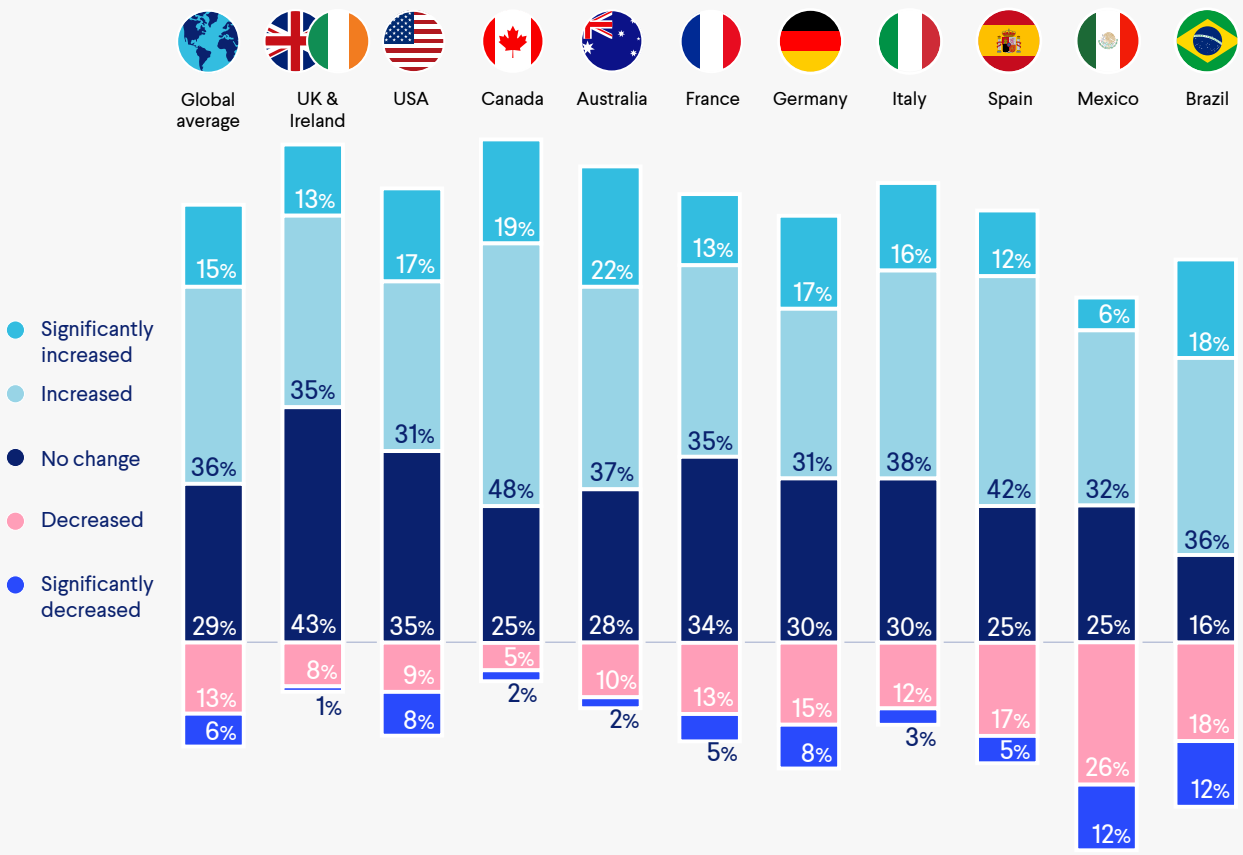
FRIENDLY FRAUD



The perception of friendly fraud levels varies greatly across regions. And the percentage of merchants that feel levels have stayed the same stands out quite a bit here. This is particularly true for UK and Irish merchants at 50%. Could this be down to more lenient refund and return policies?

On the upper end, around 60% of Australian merchants have seen an increase. Meanwhile, only 24% of Mexican merchants say the same. In fact, almost 50% of Mexican merchants say that friendly fraud has decreased.

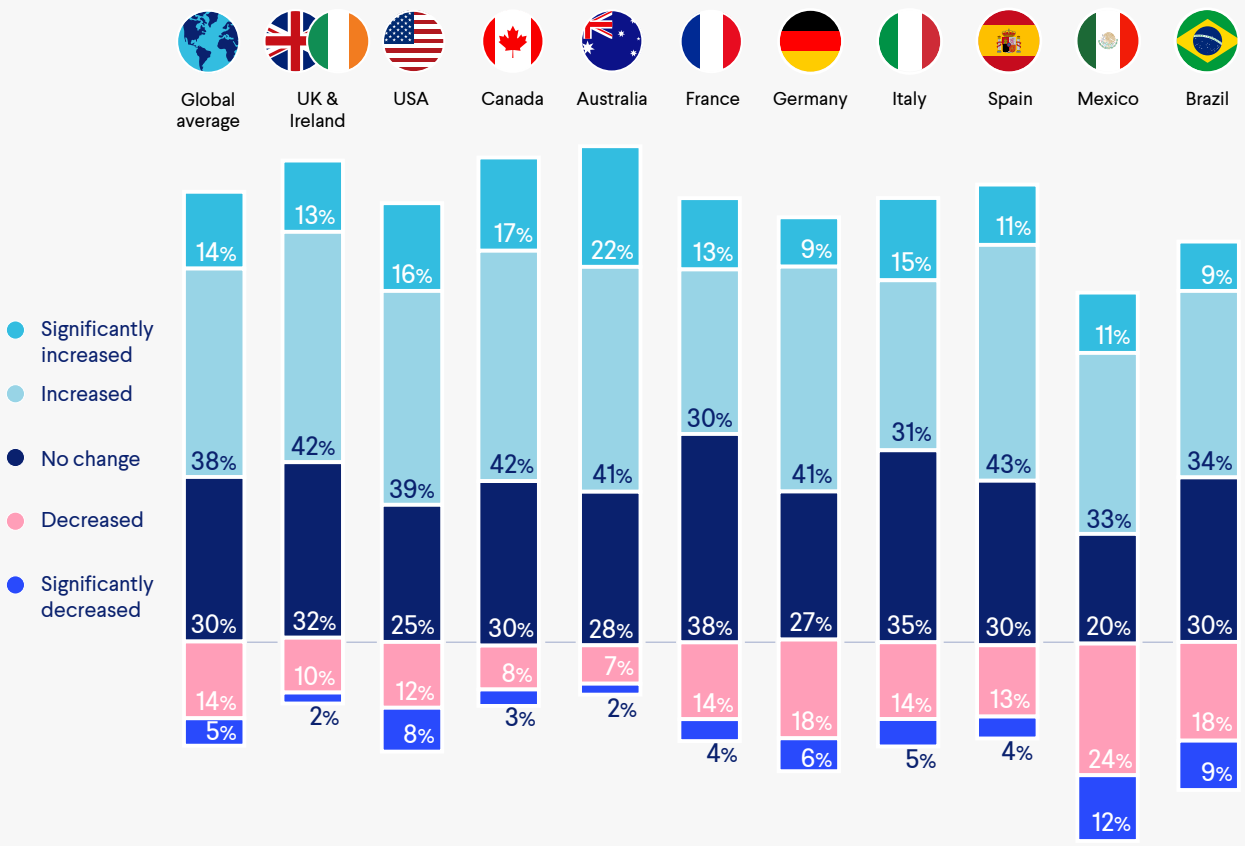
ACCOUNT TAKEOVER



Account takeover attacks are on the rise – especially for Canadian merchants. Almost 70% percent say that attacks have increased. This is well above the global average from respondents of 51%.

Canada experienced some of the **highest volumes of bot traffic in 2021.** And there is often a correlation between **bad bots and account takeover attacks.** This could be why the perception of account takeover is higher than in other regions.

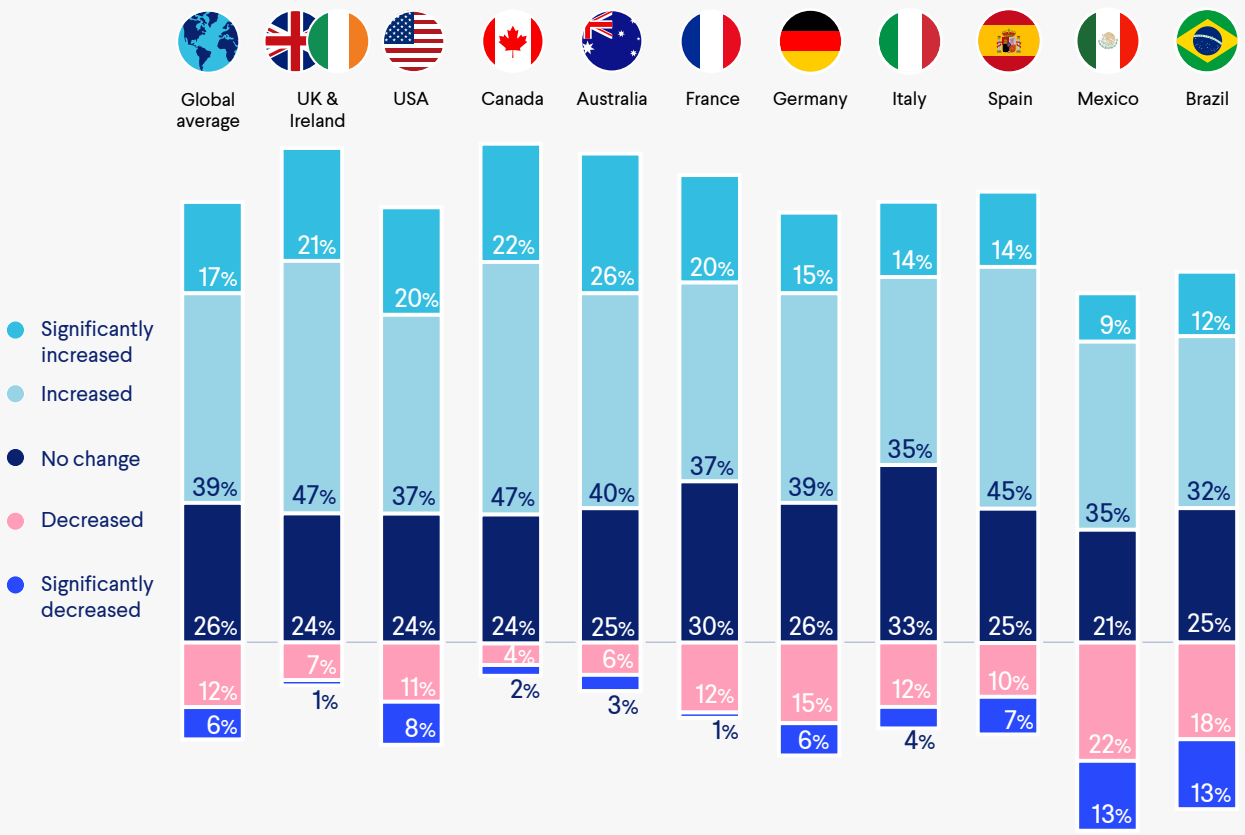
PROMOTION ABUSE



Australian merchants are the most likely to report an increase in promotion abuse at 63%. **Research into financial wellness** in the country shows that financial stress has doubled in the past two years. Consumers often turn their attention to bargains and deals when money is tight, so they're important for business. Unfortunately, this is often accompanied by an increase in promotion abuse.

Customers often see misusing discounts code, vouchers and referral bonuses **a gray area**. Especially as they're forced to cut their budgets to save money with increasing costs of living.

RETURNS / REFUND ABUSE

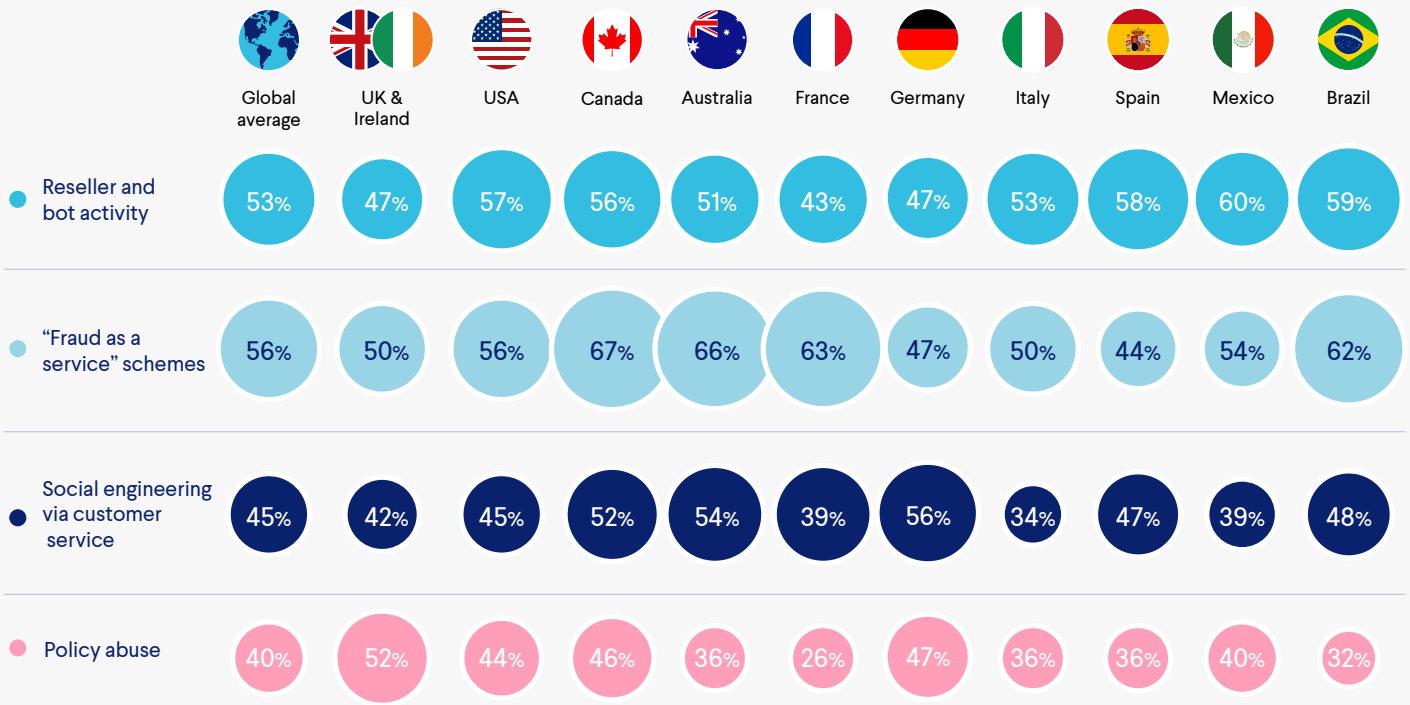


Refund/returns abuse seems to be the fastest growing fraud threat after online payment fraud. Almost 70% of Canadian, Australian and UK and Irish merchants have seen an increase. As mentioned, genuine customers are more likely to try their luck in difficult financial times.

Then you have fraudsters. They very quickly find new points of entry when companies tighten up their defenses. Refund fraud is outright malicious organized fraud for profit. We're notably seeing its costly rise in relation to **fraud as a service**. Professional refunders are using social media to offer their services to legitimate customers looking for a bargain.

ARE YOU BEING HIT BY NEW FRAUD TYPES?

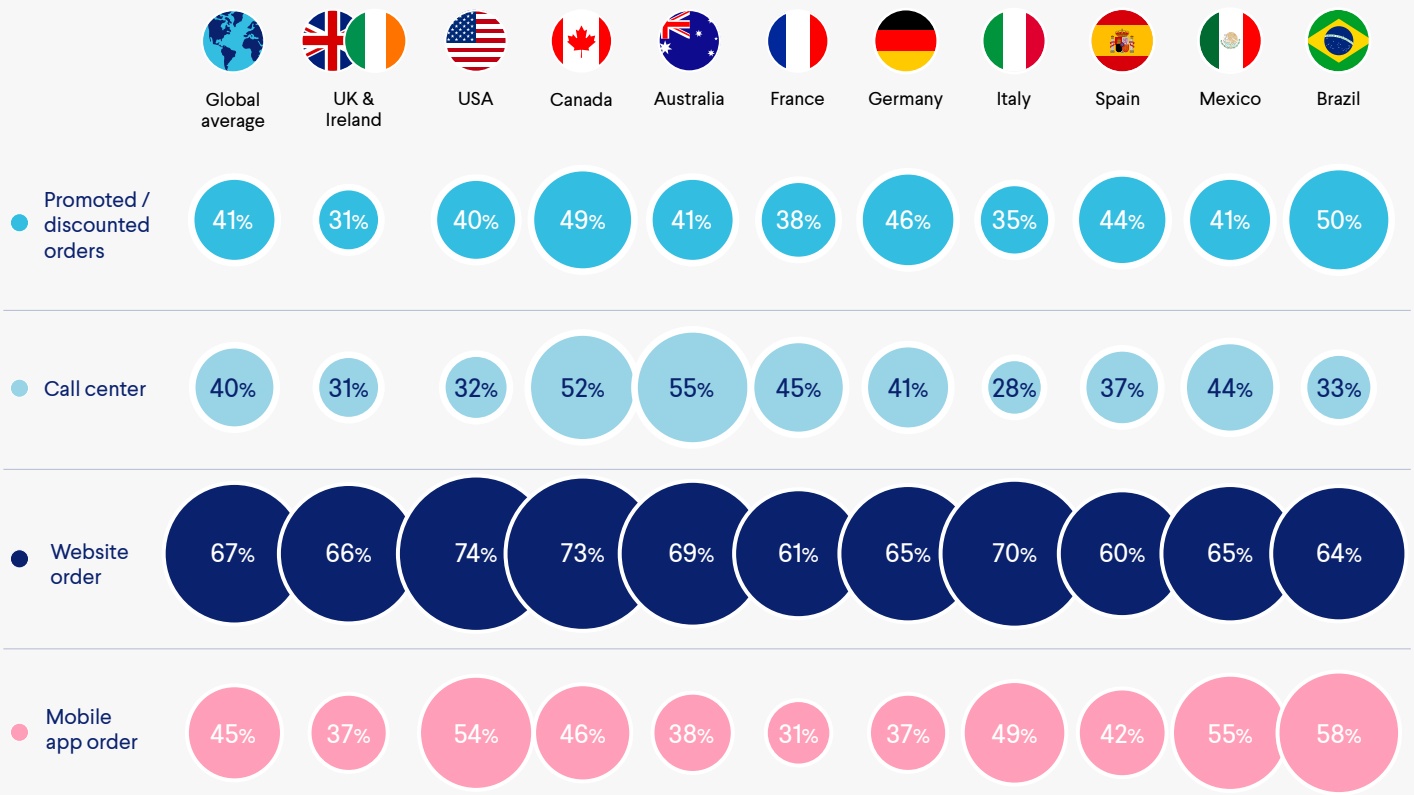
WHAT ARE SOME OF THE NEW TYPES OF FRAUD TRENDS THAT YOUR BUSINESS IS SEEING?



The increase in the "newer" types of fraud is consistent globally. This reflects the scale and reach of emerging fraud trends. The internet has facilitated the spread of knowledge and ideas, and unfortunately fraud is not exempt. Fraudsters are able to use social media channels and platforms to teach others how to bypass security measures. What are fraudsters saying about your business?

WHERE DO YOU SEE THE MOST FRAUD?

ON WHICH ORDER TYPES DO YOU SEE THE MOST FRAUD?



Website orders are the most fraudulent order type on average by quite a stretch. This isn't surprising as online purchases are typically made through the company websites.

We could soon see mobile app orders rise up the ranks as a payment method to watch out for. They are already considered problematic by almost 60% of Brazilian merchants. Mobile commerce volumes are expected to hit **$620.97 billion by 2024**. It is estimated that nearly half of all ecommerce purchases will be made using a mobile device.

Online merchants are in a tough spot. A frictionless and customer-friendly refund/returns experience is vital to meeting the **expectations of today's consumer**. And promotions are undeniably effective in encouraging loyalty, attracting new customers, and getting them to spend more. But the abuse of these policies is costly. How are you protecting your business?

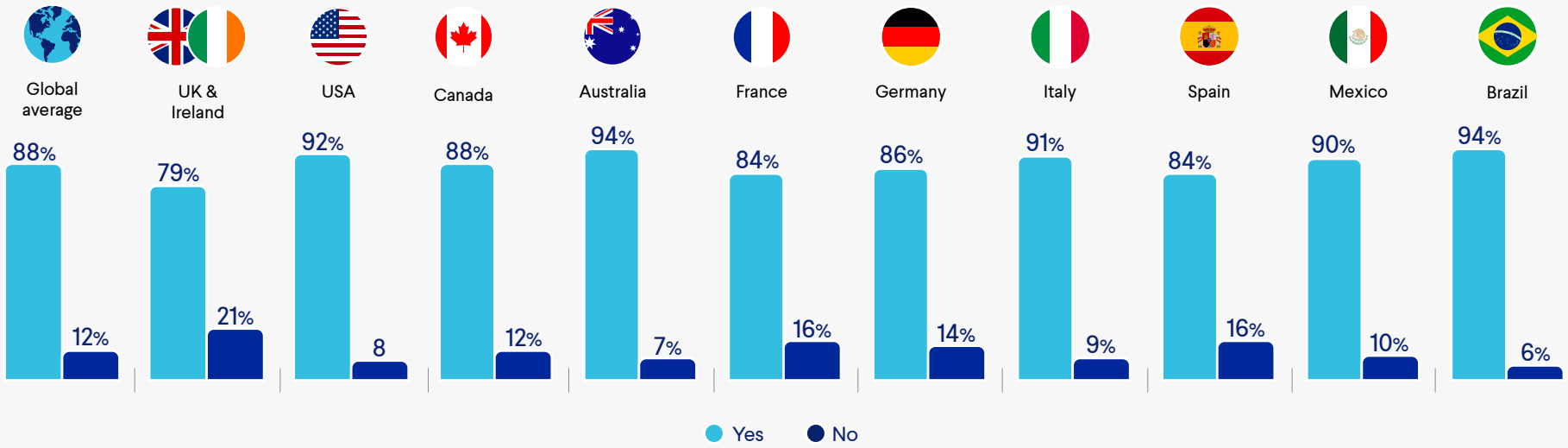
6.0
POLICY ABUSE

The rise of refunds, returns and policy abuse

Online merchants are in a tough spot. A frictionless and customer-friendly refund/returns experience is vital to meeting the **expectations of today's consumer**. And promotions are undeniably effective in encouraging loyalty, attracting new customers, and getting them to spend more. But the abuse of these policies is costly. How are you protecting your business?

ARE YOU USING TECHNOLOGY TO TACKLE POLICY ABUSE?

ARE YOU INVESTING IN TECHNOLOGY TO IDENTIFY OR PREDICT POLICY ABUSERS (REFUND, RETURNS, AND PROMOTION ABUSE)?



Policy abuse has become a hot fraud topic. This **multi-billion dollar problem** is no longer just a cost of doing business.

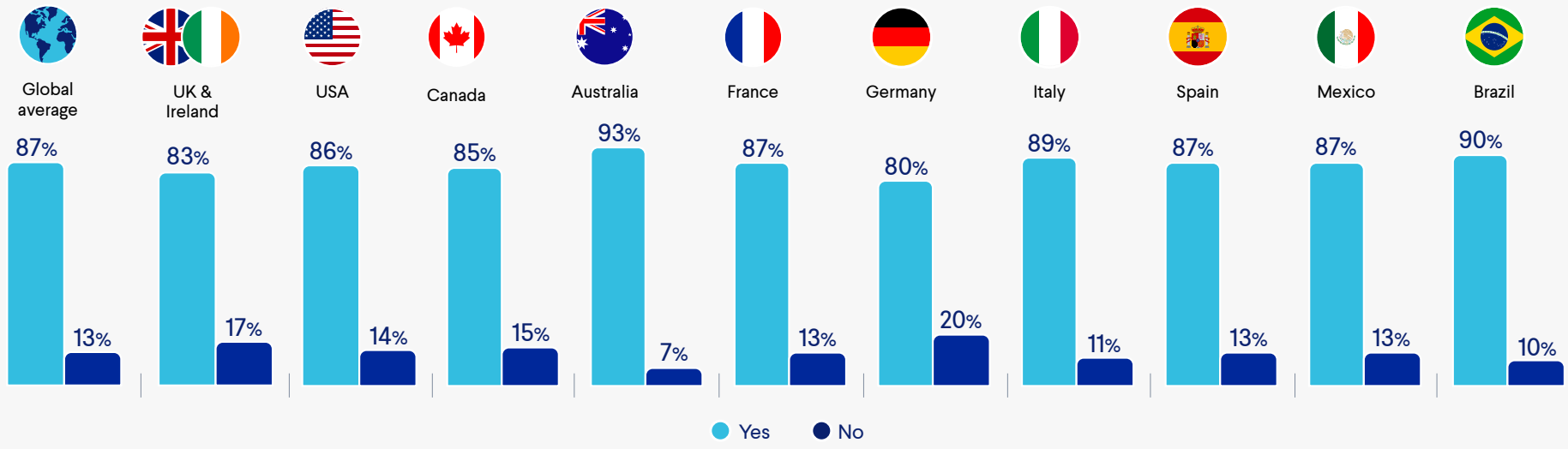
But making policies more restrictive **isn't the answer**. If you go in too strong you could actually lose customers. This is why you need a dedicated solution. Thankfully, almost 90% of merchants are investing in tools to predict and identify policy abusers.

Worryingly, just over 20% of UK and Irish merchants are not. Especially considering that almost 70% note an increase in policy abuse. Interestingly, around 50% of fraud teams from this region say refund abuse is one of their primary responsibilities after online payment fraud. Could they be relying on manual review instead?

ALMOST
90%
are investing in policy abuse tools

WHO MANAGES REFUND/RETURNS ABUSE?

IS MANAGING REFUND AND RETURNS ABUSE THE RESPONSIBILITY OF THE PAYMENT FRAUD TEAM IN YOUR BUSINESS?

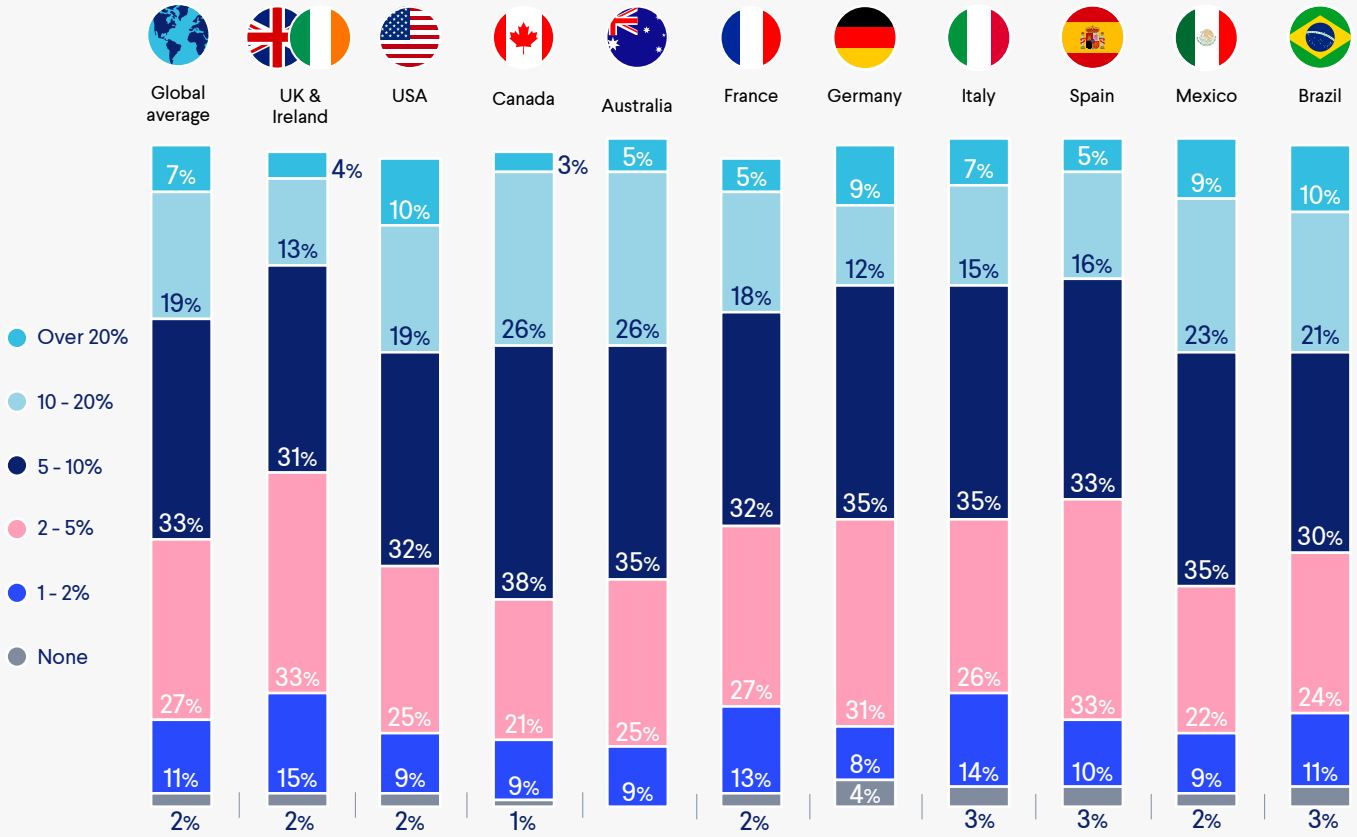


Almost 90% of merchants report that returns/refund abuse is handled by the payment fraud team. This isn't abnormal. But it is important to remember that the impact of returns/refund abuse is felt across departments.

You have to factor in the additional operational costs, like transportation and processing. It's not lost revenue you have to think about. These can amount to nearly **60% of the sale price of a $50 item**. Meanwhile, only 22% of fraud teams say they work closely with the Operations team.

HOW BIG IS YOUR REFUND/RETURNS ABUSE PROBLEM?

IN THE LAST 12 MONTHS, WHAT PERCENTAGE OF ALL RETURNS OR REFUNDS DO YOU ESTIMATE TO BE A RESULT OF ABUSE OF POLICY?



About a quarter of merchants believe that over 10% of their refunds/returns are the result of abuse. This is incredibly high and still might not offer the full picture of the problem.

So why might businesses underestimate the true cost of returns? **One reason put forward** is that few companies have a designated executive who effectively owns the refund/returns side of the business. And this includes reducing the rate of refund and returns.

As we've seen, the responsibility of handling this work falls on the payment fraud team. But that doesn't mean that it's their area of expertise. So how much are you actually losing to refund/returns abuse?

7.0 ACCOUNT SECURITY

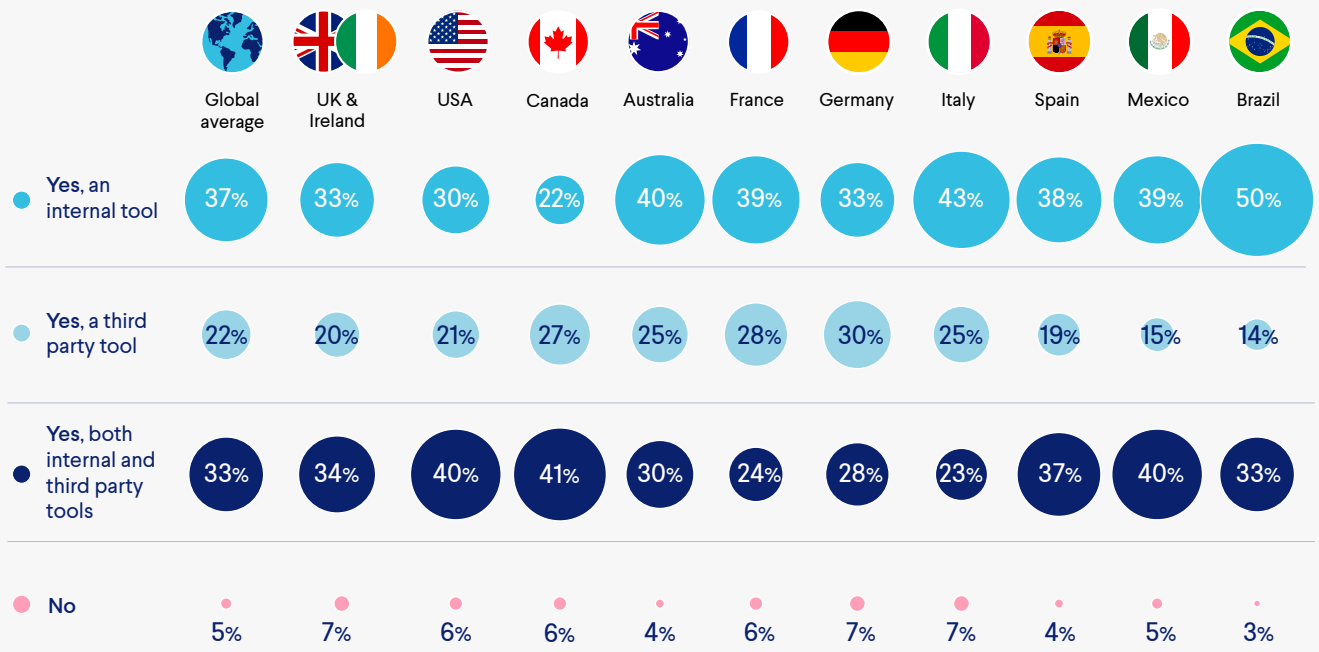
The financial and reputation risk of insecure accounts

Account takeover is the biggest fraud risk to businesses globally after online payment fraud. Around 70% of respondents say that it's a top three threat to their business. And with online retail sales set to reach over $6.5 trillion in 2023, fraud teams might have their work cut out for them.

The digital shift has created more opportunities for fraudsters to steal credentials and sensitive information. Reports show that the markets selling these credentials are robust and sophisticated. It's a whole industry in itself, complete with subscription services. Is your business feeling the sting of account takeover?

DO YOU HAVE SPECIFIC ACCOUNT TAKEOVER TOOLS?

DO YOU HAVE A SPECIFIC TOOL TO DETECT OR PREVENT ACCOUNT TAKEOVER?

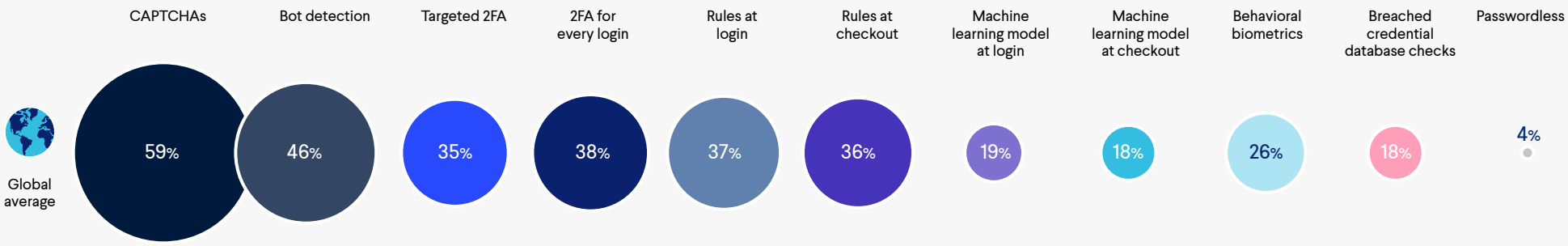


Customer accounts allow you to offer a **personalized shopping experience and a more streamlined checkout process.** This convenience and ease of purchase is great for sales. The issue is customer accounts are increasingly viewed by fraudsters as weak points to exploit.

It makes sense then that the majority of merchants across the board report using some sort of account takeover tool. But almost 40% are relying on just internal tools. This could point to a lack of established solutions available on the market. So merchants are forced to tackle the issue themselves by building their own tools.

WHAT TOOLS ARE YOU USING TO FIGHT ACCOUNT TAKEOVER?

DO YOU CURRENTLY USE ANY OF THE FOLLOWING FUNCTIONALITY OR TOOLS AS PART OF YOUR STRATEGY TO MITIGATE ACCOUNT TAKEOVER FRAUD?



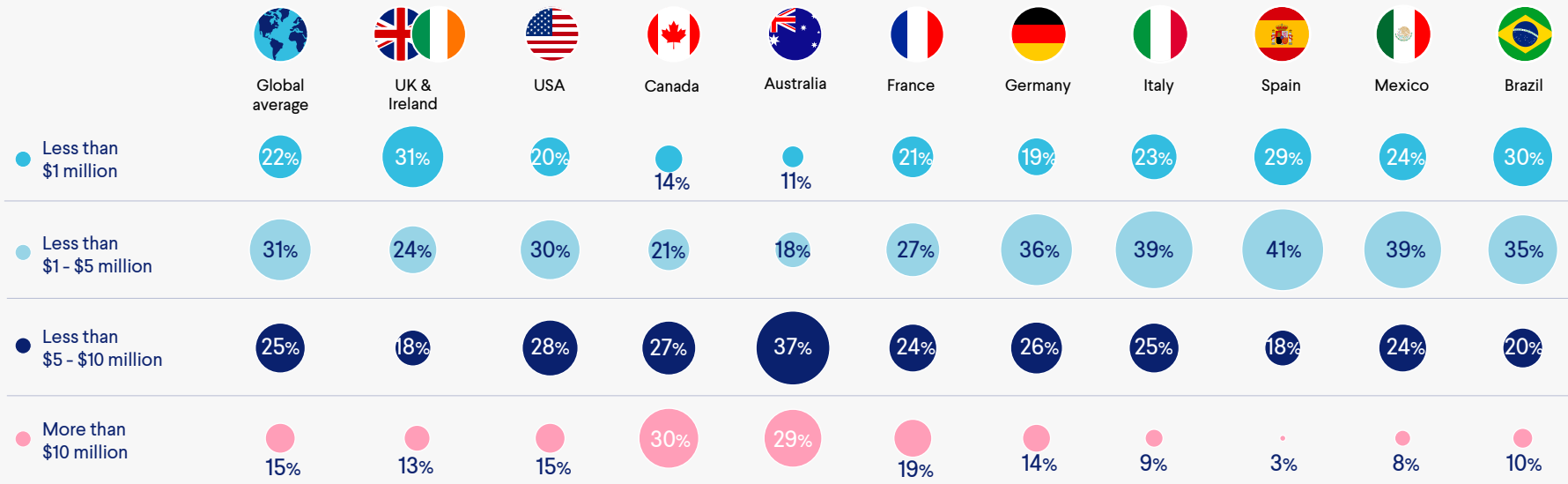
So what specific tools are merchants using to protect their customer accounts? Interestingly, there wasn't much variation between regions in terms of the solutions they preferred. So the global averages are reflective of the responses from each country. If anything, what stands out is how few merchants report using each of these tools.

Take, for example, bot detection. Credential stuffing is **one of the leading types of malicious bot attacks**. This brute force attack allows criminals to test thousands of stolen credentials on your site in an instant. So while bot detection is the second most popular tool, it's concerning that less than half of merchants are putting it to use.

The percentage of merchants that report using machine learning is very low at under 20%. But **machine learning for account takeover** protects customers without disturbing their shopping experience. Custom models factor in what's normal behavior for your customers across all points of their journey. This means you can easily identify potential takeover attempts at login and checkout, and react proactively.

HOW MUCH ARE YOU LOSING TO ACCOUNT TAKEOVER?

ROUGHLY HOW MUCH DOES ACCOUNT TAKEOVER COST YOUR BUSINESS ANNUALLY?

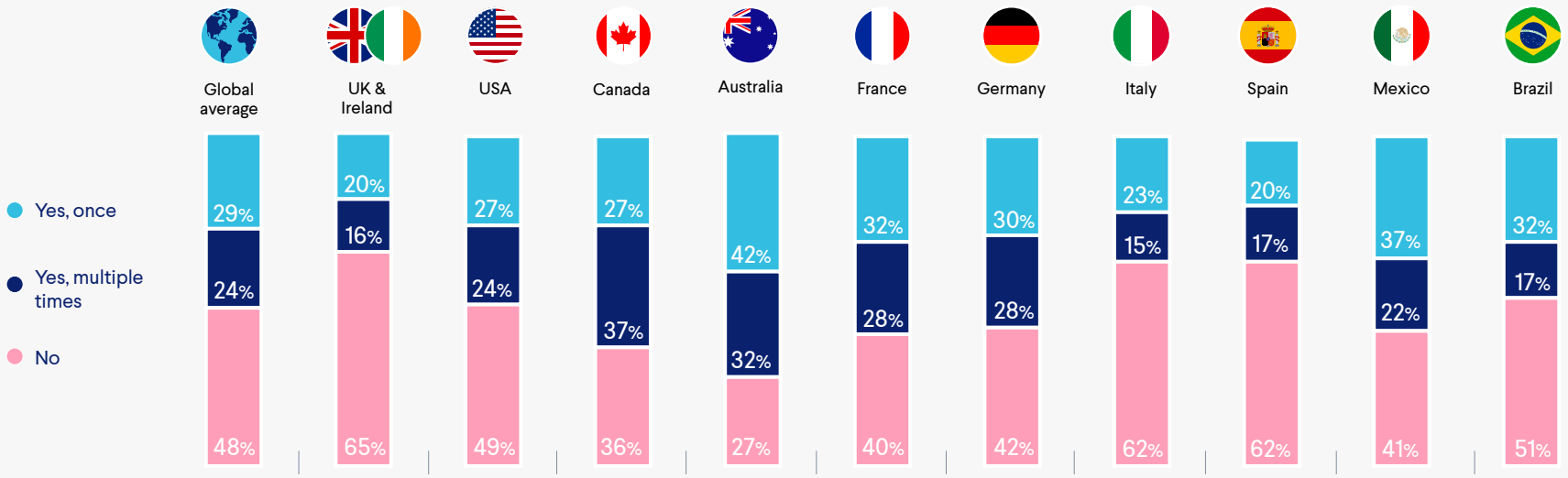


On average, over 50% of merchants globally say they lose up to $5 million a year as a result of account takeover. This is no small sum, but the total financial impact of this type of fraud isn't always immediately obvious. The reputational damage and loss of user confidence that follows an attack is a huge threat to your bottom line.

Notably, around a third of Canadian and Australian merchants say that account takeover costs their businesses north of $10 million annually. As we've already mentioned, Canadian merchants were the most likely to report an increase in account takeover attacks at around 67%.

HAS YOUR ACCOUNT TAKEOVER PROBLEM HIT THE PRESS?

IN THE PAST 12 MONTHS, HAS YOUR COMPANY BEEN FEATURED IN THE PRESS OR SOCIAL MEDIA BECAUSE OF ACCOUNT TAKEOVERS?



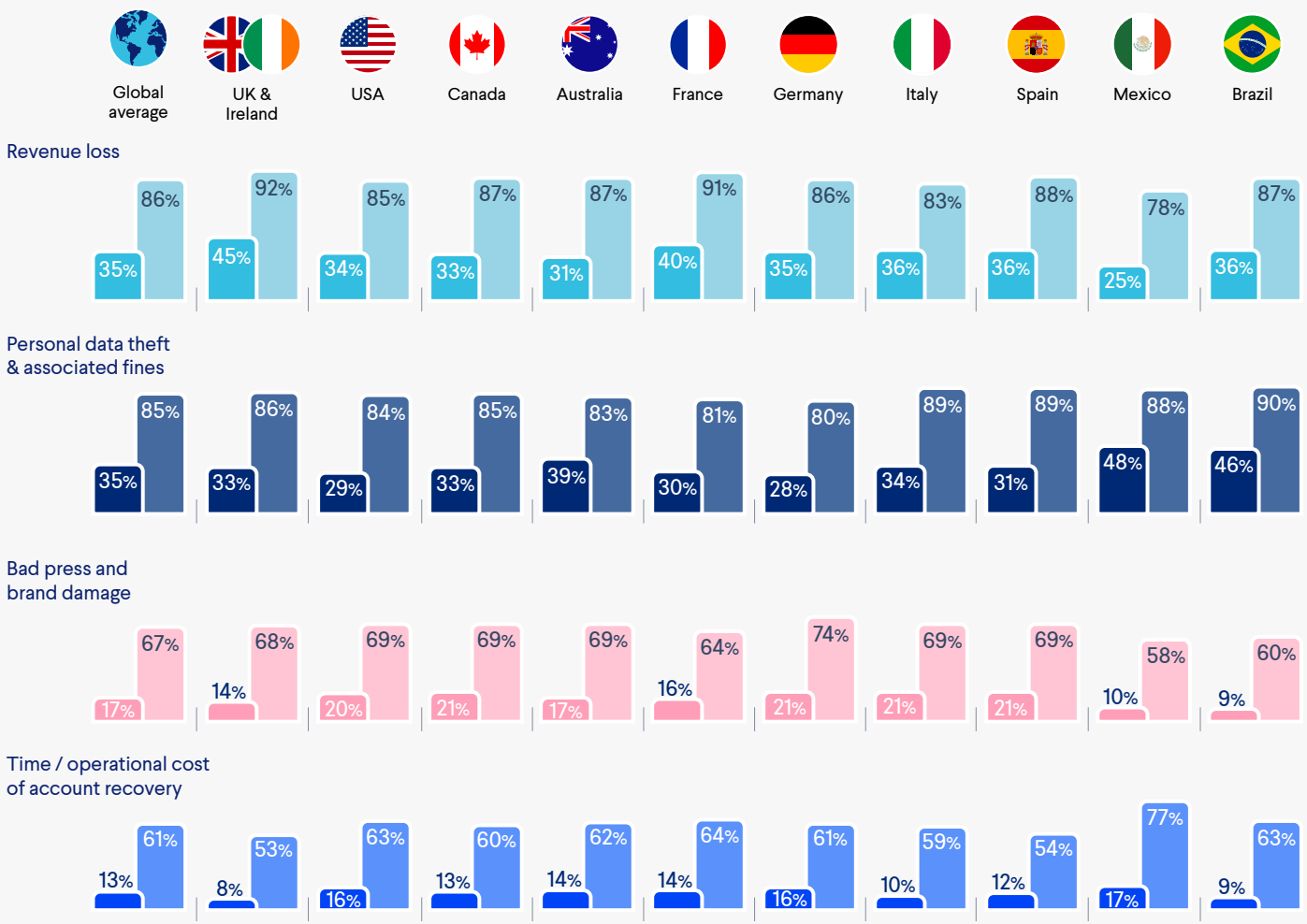
Over half of merchants say they have been in the press at least once in the past year because of account takeover. Almost a quarter have been featured more than once, which is quite significant.

The reputational impact of a public account takeover attack on your site cannot be overstated. **Customer loyalty is severely threatened when consumers experience fraud.** And it doesn't help that the ecommerce market is so saturated that customers are spoilt for choice. You could end up losing existing valued customers and future customers to a competitor.

53%
have been in the press for ATO

WHAT BUSINESS IMPACT ARE YOU MOST CONCERNED ABOUT?

WHAT ARE THE MOST IMPORTANT RISK FACTORS WHEN CONSIDERING THE COST OF ACCOUNT TAKEOVER ON YOUR BUSINESS?



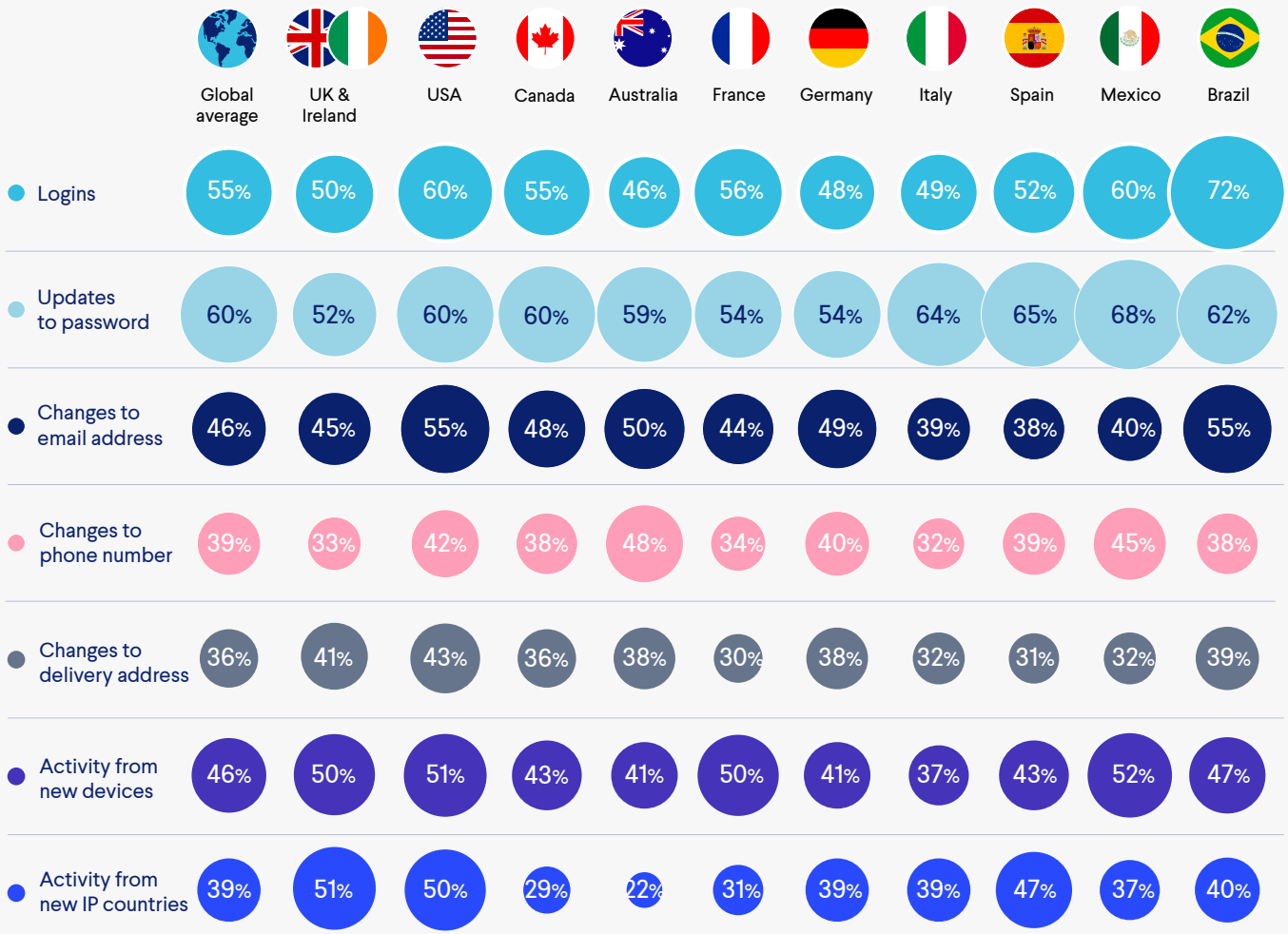
The fallout of an account takeover attack on your business is huge. But what are merchants most worried about? Similar to last year, merchants seem most concerned about the threat to their wallets.

More specifically, it's revenue loss and the fines associated with data theft that have them up at night. On average 35% of merchants globally say that these are the number one risks to their business when it comes to account takeover.

Merchants seem slightly less worried about negative publicity and the operational costs of account recovery. But these threats also carry their own longer-term financial risks.

WHAT ACTIVITY ARE YOU TRACKING TO PREVENT ATTACKS?

DO YOU MONITOR ANY OF THE FOLLOWING AS PART OF TACKLING ACCOUNT TAKEOVERS?

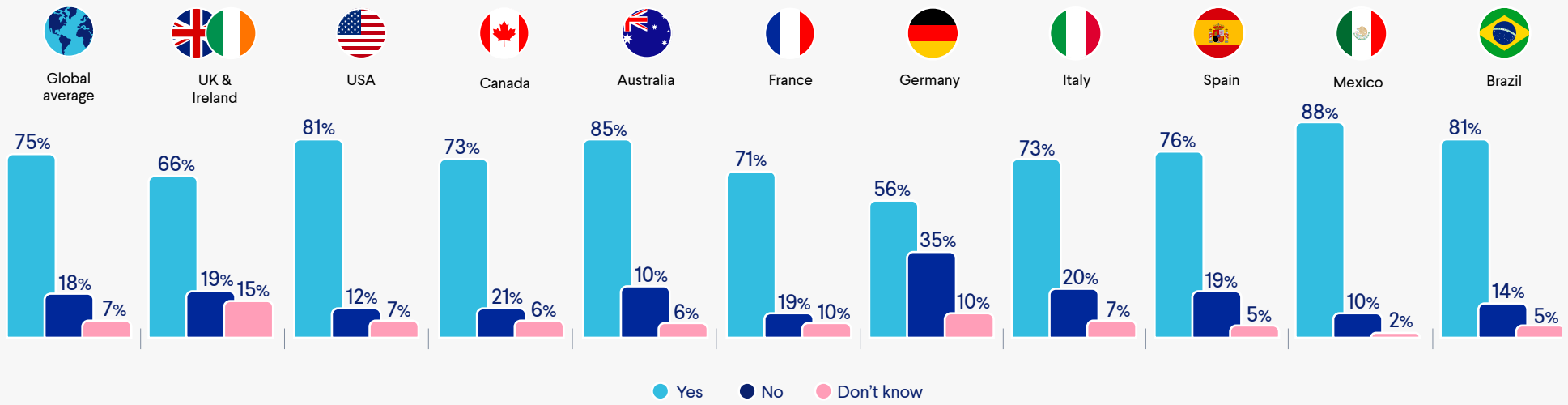


Monitoring customer activity should be top of your list of actions. Feedback shows that merchants are keeping an eye on a wide range of activities. But the percentage of merchants who actually report tracking each of these behaviors is very low.

Sudden changes in customer behavior could point to a snake in the grass. So you could be missing a trick. This information informs what you do next – are there rules you can put in place? What is the risk score for this transaction?

HOW ARE YOU GETTING BACK CUSTOMER ACCOUNTS?

DO YOU HAVE A DOCUMENTED PROCESS FOR REACTIVATING ACCOUNT TAKEOVER VICTIM ACCOUNTS?



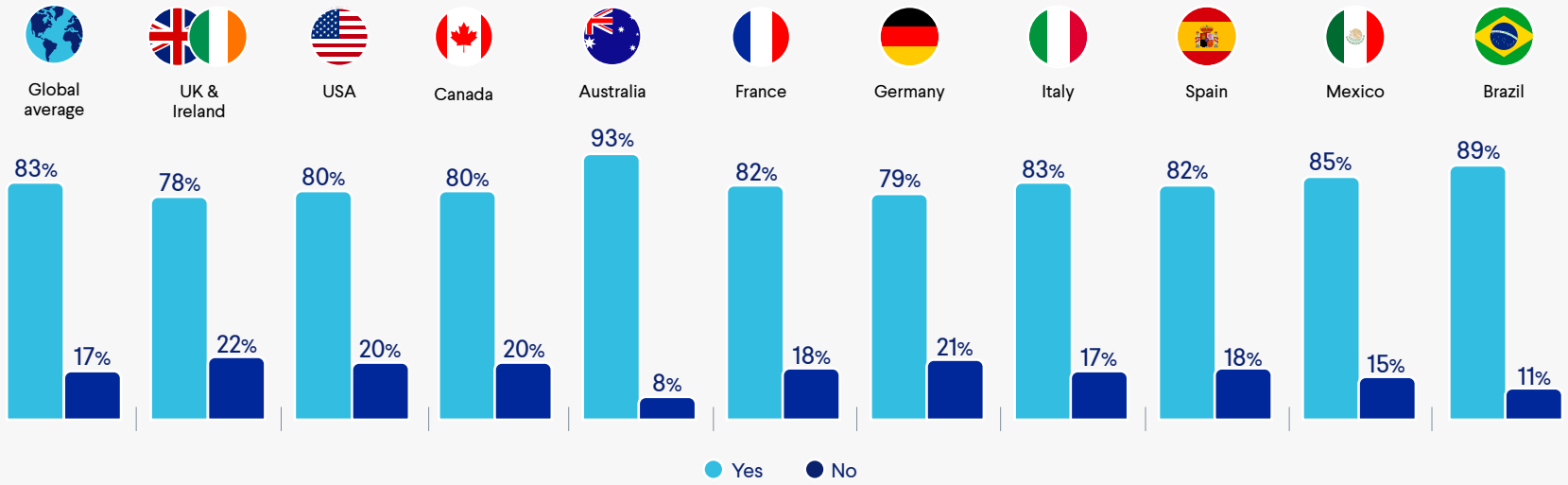
Most merchants have a documented process for recovering accounts, which is good to see. But you'd hope that this figure would be greater. Almost 20% of merchants don't have one at all, which is shocking.

These accounts are valuable to your customers and the relationship you have with them. Incentives like loyalty programs are a **powerful motivation for buyers to create accounts, come back, and spend more.**

What's more, **trust is so important in ecommerce.** Your customers need to know that you will look after their personal information. And in the case that this is compromised, they need reassurance that you will rectify the situation quickly.

ARE YOU MAKING USE OF A BREACHED CREDENTIAL DATABASE?

DO YOU CHECK CUSTOMER ACCOUNT LOGIN DETAILS AGAINST A BREACHED CREDENTIAL DATABASE?



There were reportedly **over 24 billion credentials circulating on the dark web in 2022.** And this number will undoubtedly have gone up. So there's definitely value in checking credentials against a breached credential database. And over 80% of merchants are doing just this.

But you can't rely on this alone. By the time the credentials reach the database, they're already out of date and the fraudsters have moved on. Stolen data is relatively accessible on the dark web, so it really is a race against time. Case in point – a fraudster marketplace **released over 1.2 million stolen credit card credentials** in 2022.

You're still vulnerable to the new data that professional sophisticated hackers will be using. But using a breached credential database can make life difficult for more opportunistic low-tech fraudsters.

8.0 DISPUTE MANAGEMENT

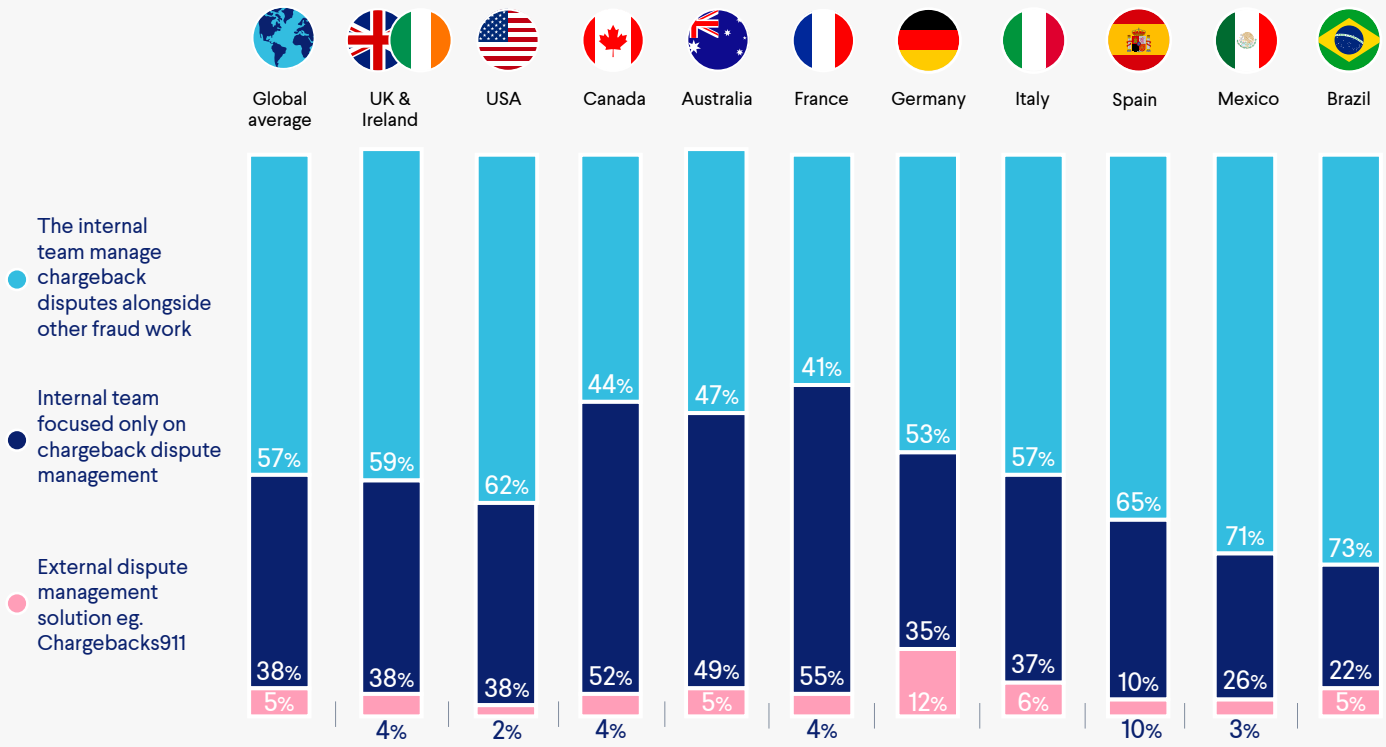
Challenge and success rates

Chargebacks are a serious business. It's not just fees you have to worry about. There are a host of additional hidden costs that'll do a number on your bottom line. Estimates vary widely, but a **report based on 611 million chargebacks** put this figure at $117 billion in 2021. And merchants stand to pay $78 billion of that total.

The cost to your business is huge. And how you calculate this has massive implications. Whatever approach you take, there is no question that developing a strategy to dispute invalid chargebacks can save your business millions of dollars.

HOW DO YOU HANDLE DISPUTES?

WHAT BEST DESCRIBES YOUR DISPUTE MANAGEMENT RESOURCE?



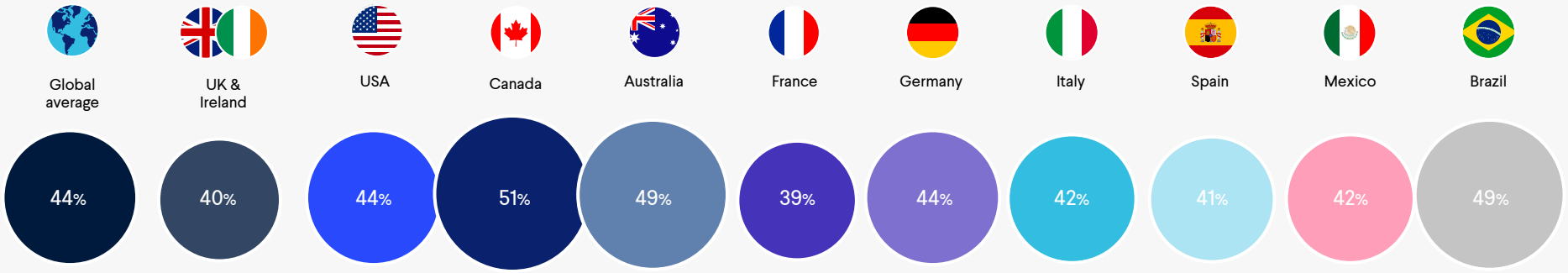
So how are merchants handling this work? For the most part, merchants globally seem to be relying on an internal team who manages disputes alongside other fraud work. This might work well depending on the scale of disputable chargebacks your business might have.

Canada, Australia and France disproportionately report having an internal team that focuses on dispute management alone. A surprisingly low number of respondents report using an external provider of which there are many.

ARE YOU SUCCESSFULLY CHALLENGING ILLEGITIMATE DISPUTES?

Disputes are to be expected, but not all of them will be legitimate. So letting them slide could wind up costing you a fortune. We wanted to find out what percentage of disputes merchants are challenging. And just how successful they are at doing it.

ON AVERAGE, WHAT PERCENTAGE OF CHARGEBACKS DO YOU CHALLENGE?



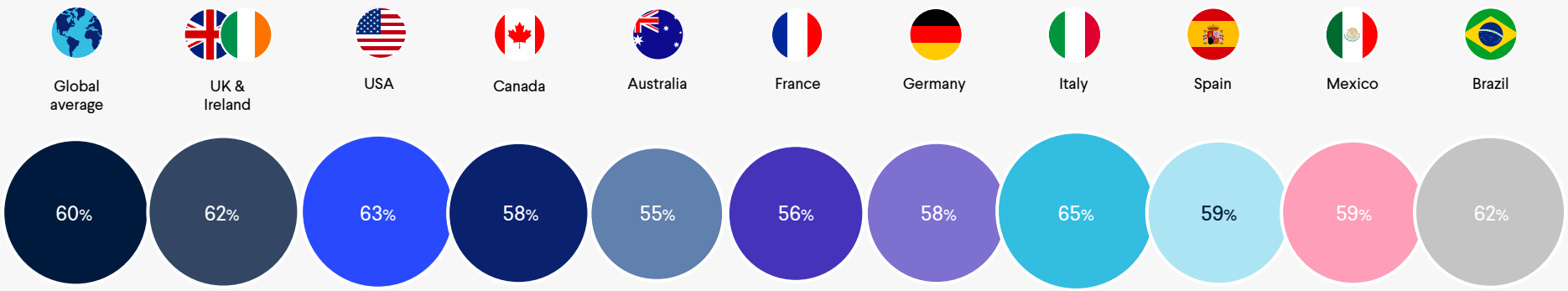
While there isn't much variation between regions - on average merchants are challenging 44% – the global number of challenged chargebacks is still very high. In some ways, this really paints a picture of the size of the first-party fraud problem.

Of course, there are other reasons for chargeback disputes, like **poor merchant visibility** on bills. But not having a solid dispute management process will leave you wide open to loss.

44%

Global average of chargebacks challenged

WHAT IS YOUR SUCCESS RATE WHEN CHALLENGING DISPUTES? OF ALL THE DISPUTES YOU CHALLENGE, WHAT PERCENTAGE ARE YOU SUCCESSFUL WITH?



Of the disputes they challenge, respondents say they're successful on average 60% of the time. This figure was 66% in 2021. This slight drop could be related to the increasing popularity of new payment methods. As we'll see, challenging new payment methods cause merchants the most trouble. But in any case, it shows that a challenge is worthwhile two times in three. So worth the investment by any measure!

Merchants report a

60%

SUCCESS RATE

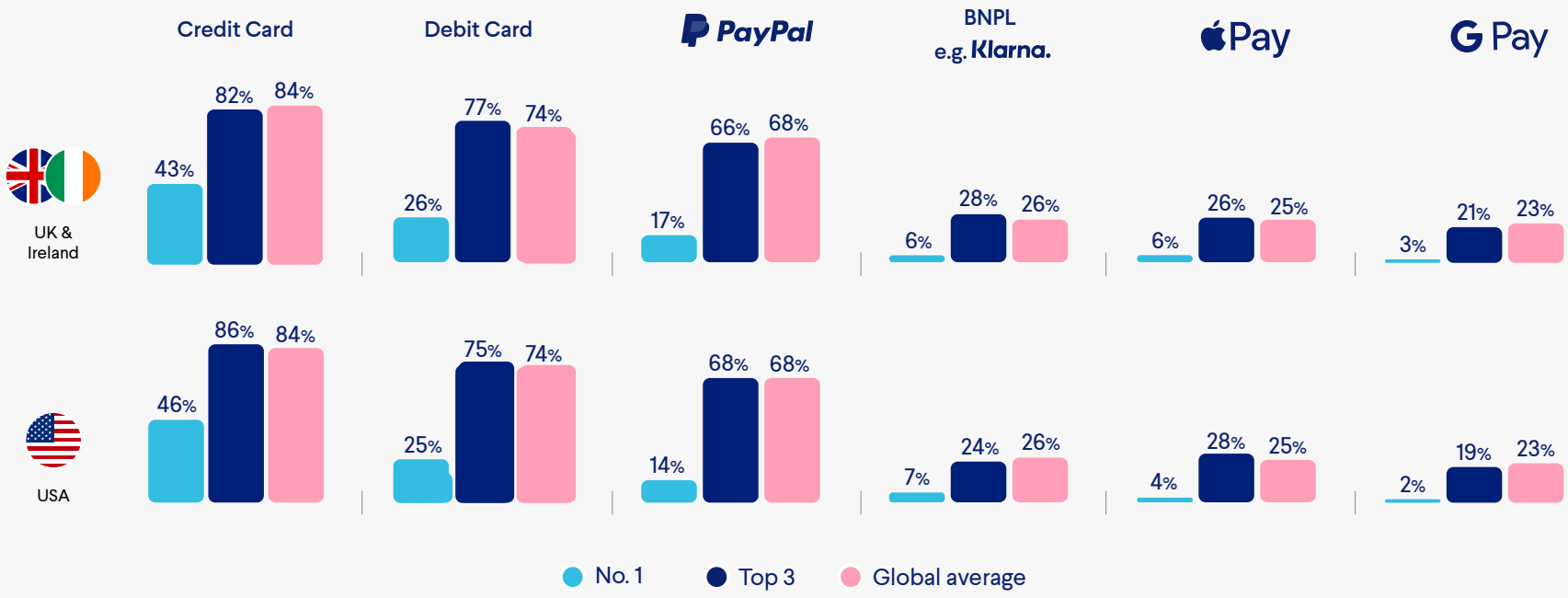
WHICH PAYMENT METHODS ARE EASIEST TO CHALLENGE?

We asked merchants for the top three payment methods that they challenge most successfully. On average, around 80% of merchants said credit and debit card payments were in their top three. This result isn't wholly unexpected – most merchants are familiar with the process when it comes to traditional payments.

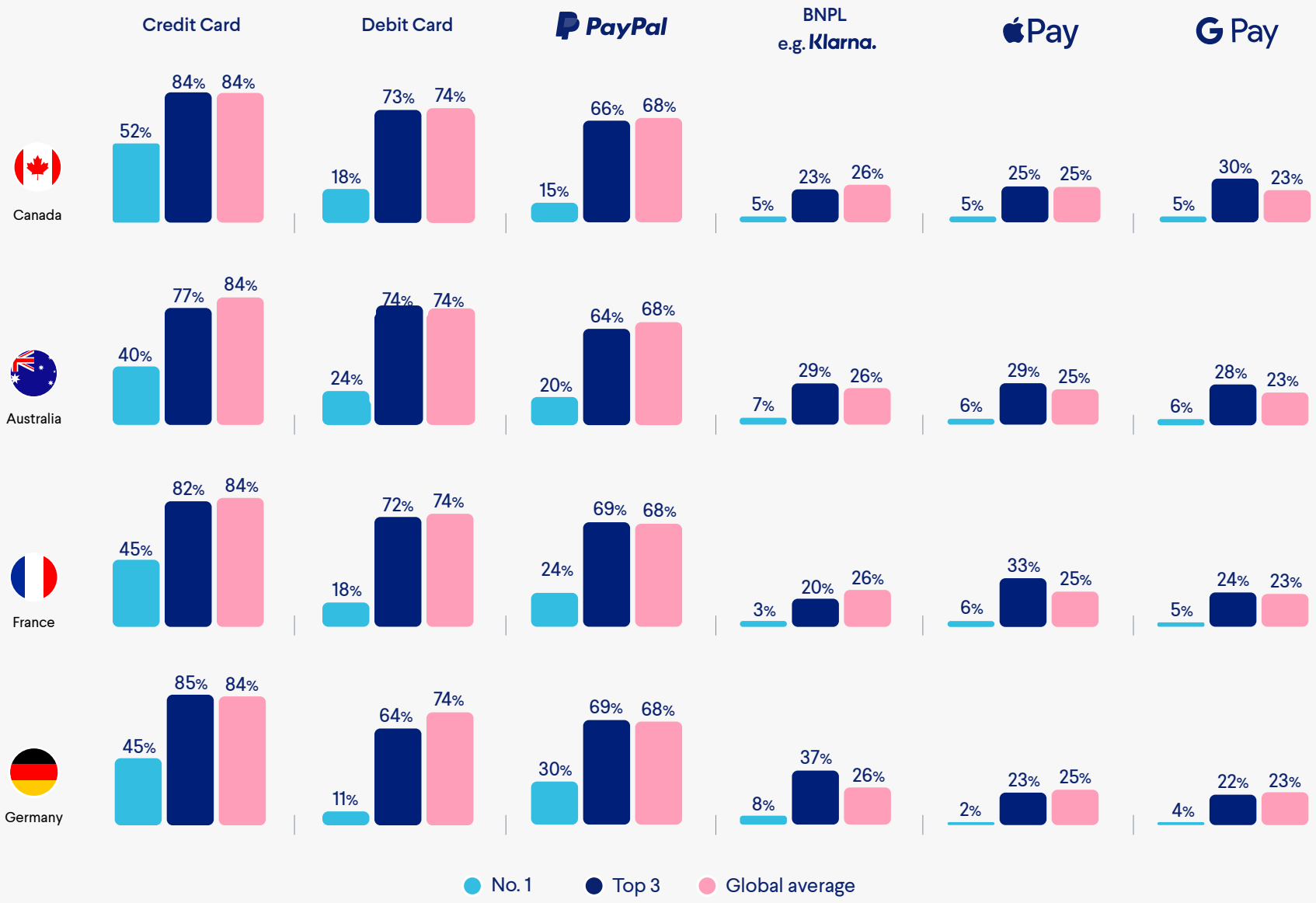
Wallet payment challenges were much less successful. Lack of familiarity is possibly why merchants seem to find newer payment methods trickier. Before you challenge a dispute, you need to consider two things: how easy is it to collect the evidence you need to build a case? And, how likely is your challenge to be accepted?

Unfortunately, with these latest payment methods some customer payment information is obscured, making it more difficult. We will likely see the success rates start to converge as they become the mainstream.

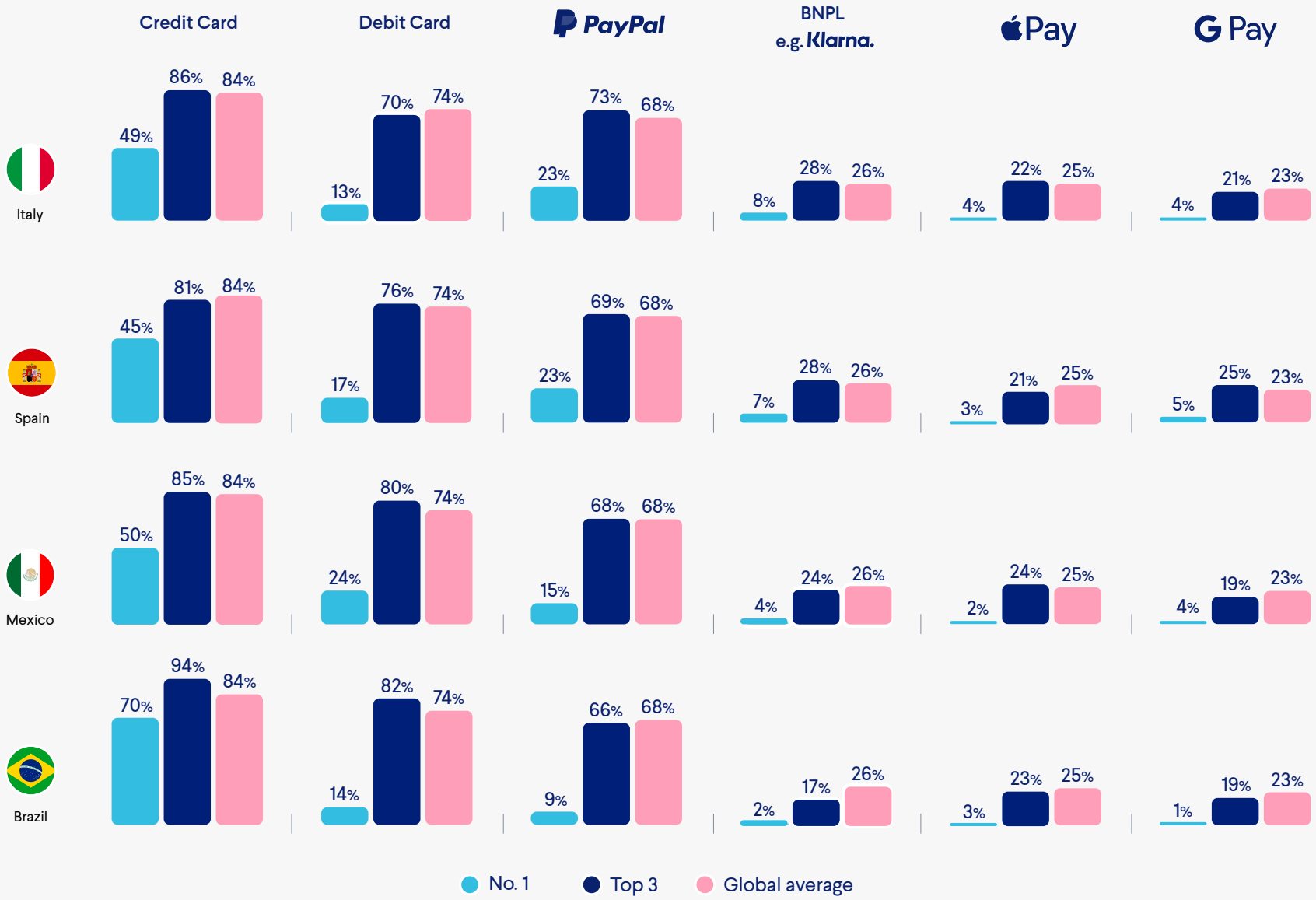
WHICH ARE THE TOP THREE PAYMENT METHODS YOU SEE THE MOST SUCCESS WITH WHEN CHALLENGING CHARGEBACKS?



WHICH ARE THE TOP THREE PAYMENT METHODS YOU SEE THE MOST SUCCESS WITH WHEN CHALLENGING CHARGEBACKS?



WHICH ARE THE TOP THREE PAYMENT METHODS YOU SEE THE MOST SUCCESS WITH WHEN CHALLENGING CHARGEBACKS?



9.0 PSD & AUTHENTICATION

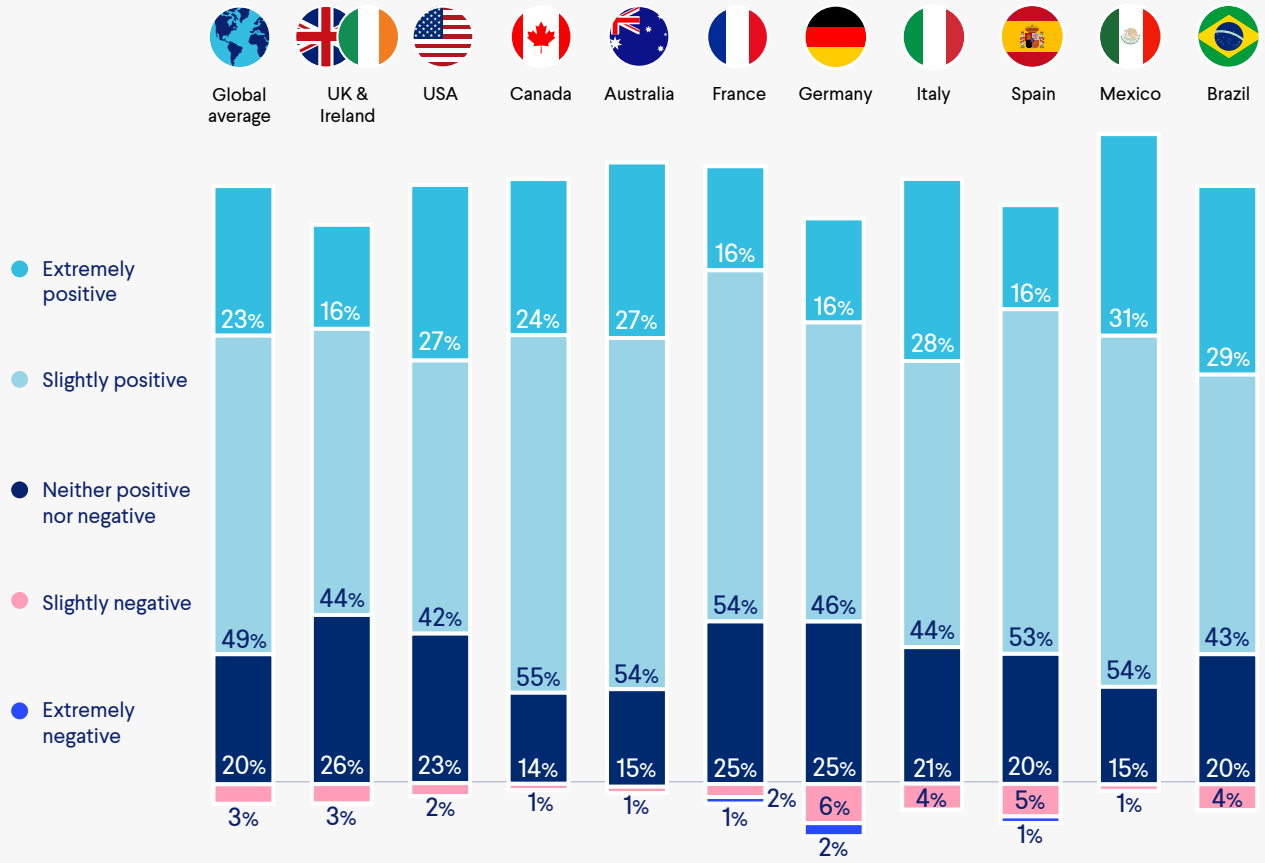
The impact of PSD2 and growing use of authentication

Maximizing acceptance rates is a constant goal in ecommerce. So it's been a particularly interesting time with the introduction of PSD2 in Europe in September 2019. The journey hasn't exactly been smooth but full compliance was reached in March 2022.

As a result, we've been able to watch as a very large economic area experiments with SCA. So what are merchants reporting after **initial scare stories** about the impact on customer experience and consequent damage to acceptance rates?

HOW ARE YOU FEELING ABOUT THE IMPACT OF PSD2 ON BUSINESS?

DO YOU VIEW PSD2 LEGISLATION AS HAVING AN OVERALL POSITIVE OR NEGATIVE IMPACT ON YOUR BUSINESS?



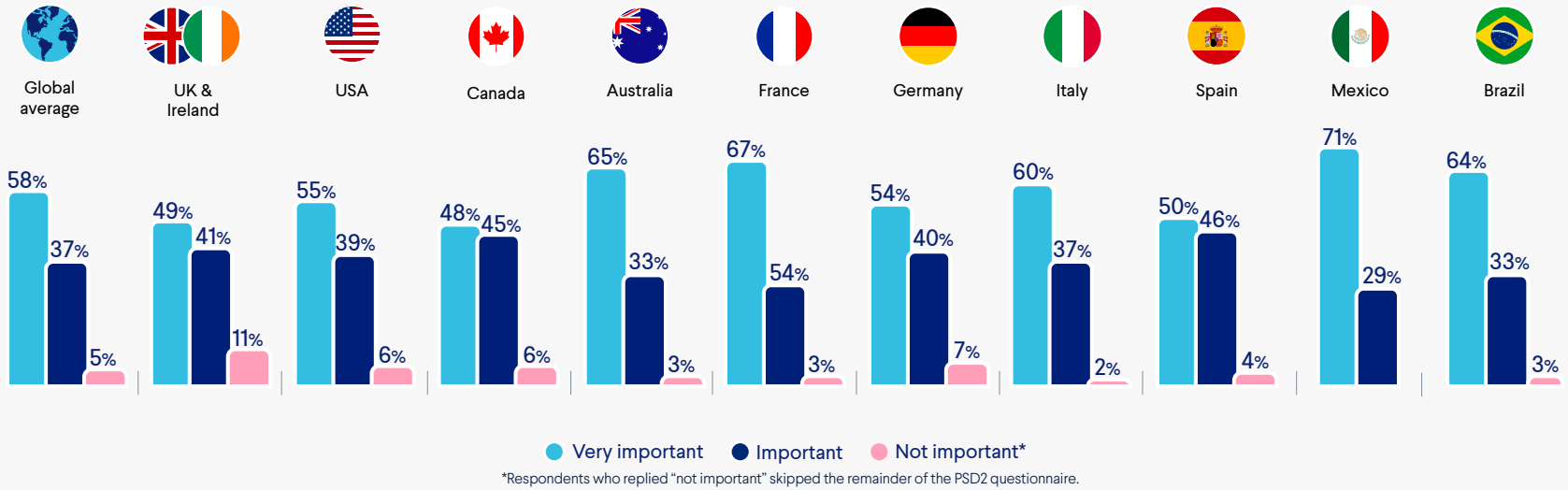
How are merchants feeling about PSD2 now? On average, around 70% of merchants across regions believe that PSD2 has had a positive impact on business.

According to the European Banking Authority (EBA), the **regulation is doing its job**. They found that the share of fraud by value for payments authenticated with SCA is three times lower than those authenticated without.

Even so, European merchants are the least likely to view the impact of PSD2 as “extremely positive”. Their more tempered view could be from direct experience. And the very real concern that SCA may create “a **lack of financial inclusion** for vulnerable and non-tech savvy citizens”.

IS 3D SECURE A KEY PART OF YOUR FRAUD STRATEGY?

HOW IMPORTANT IS 3D SECURE TO YOUR FRAUD PREVENTION STRATEGY?



*Respondents who replied "not important" skipped the remainder of the PSD2 questionnaire.

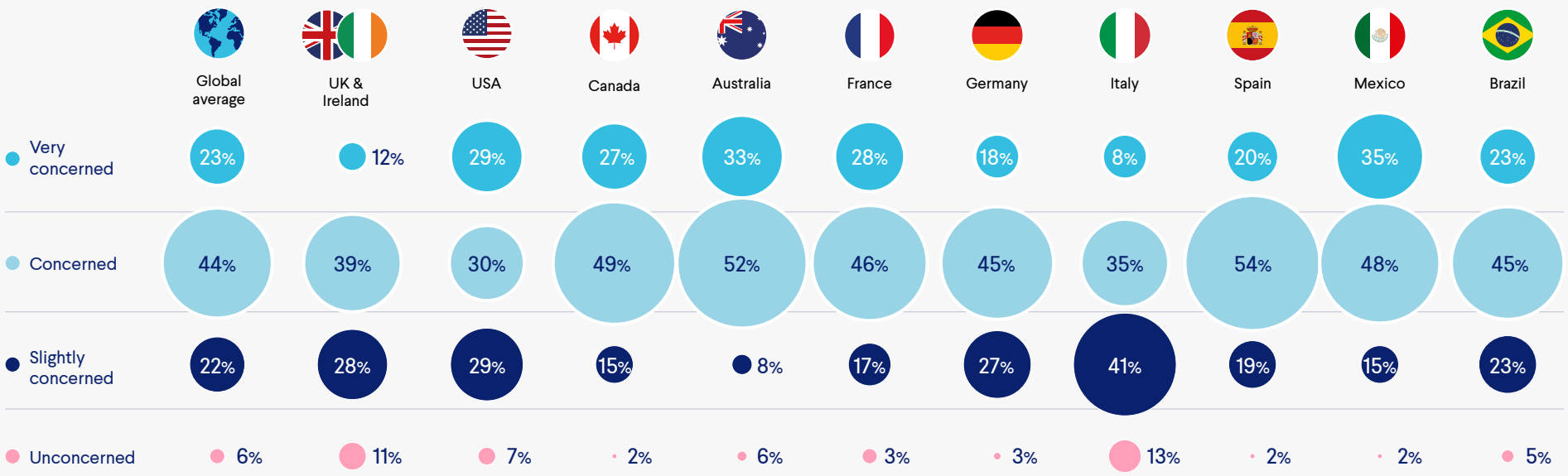
The majority of merchants consider 3D Secure (3DS) "important" or "very important" to their fraud prevention strategy.

3DS is the industry standard when it comes to authentication. So it's the obvious choice if you're looking to meet SCA requirements. Still, it's encouraging to see that it's so relevant to the prevention strategies of merchants outside the EEA.

The promise of shifting liability back onto issuers has always been appealing. But early 3DS versions were clunky and a nightmare for conversion. Fortunately, **3DS2 has swooped** in to offer better customer experience and frictionless payments. These improvements seem to have given merchants outside of Europe good reason to jump on the bandwagon.

IS 3D SECURE BAD FOR CONVERSION?

HOW CONCERNED ARE YOU ABOUT THE IMPACT OF 3D SECURE ON CONVERSION?



Balancing conversion will always be the thorn in the side of the fraud team. Friction is your friend when it comes to deterring fraud, but you can't risk putting off customers. Luckily, the latest versions of 3DS claim to provide the best of both worlds.

So do merchants believe that they can have their cake and eat it? Well, the short answer is no. Over 90% of merchants across regions are worried about what 3DS means for conversion to some degree. Almost a quarter would say that they're "very concerned".

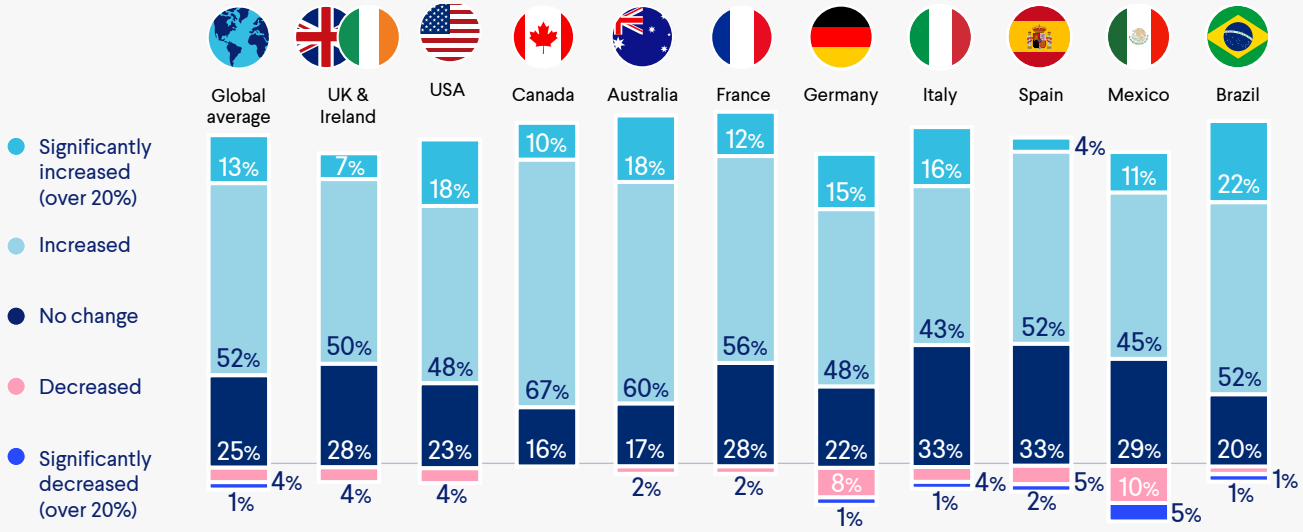
This worry could all come down to the novelty of these protocols. **3DS1 met its end last year**. And merchants are slowly trying to get their heads around version 3DS 2.1 and 2.2. Let's not even begin to discuss 2.3! It's hard to keep up with the speed at which versions are introduced and others become obsolete.

Lack of readiness in the early days of 3DS saw an expensive surge in failed transactions and **high cart abandonment rates**. So it's important to stay up to date.

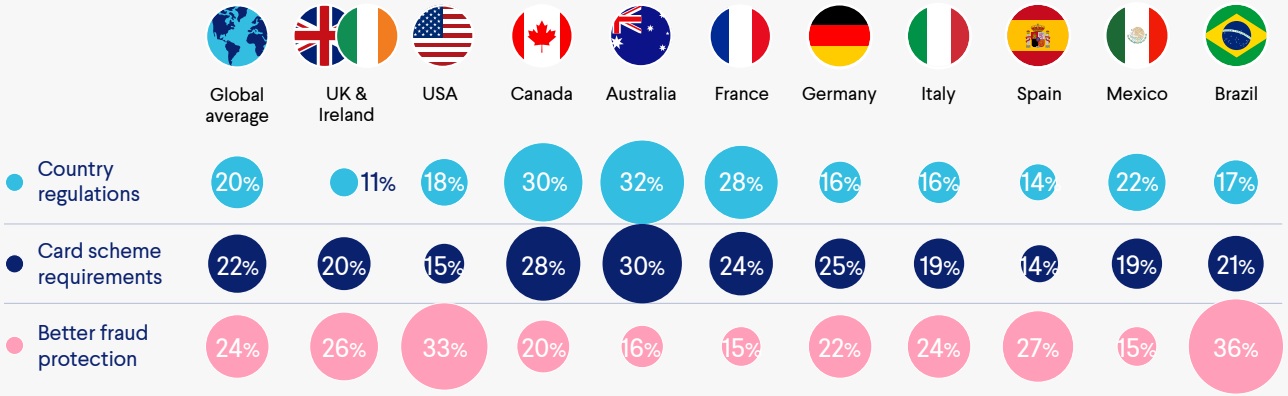
OVER
90%
are concerned about the impact on conversion

HOW MUCH TRAFFIC ARE YOU SENDING TO AUTHENTICATION?

IN THE PAST 12 MONTHS, HOW HAS THE AMOUNT OF TRAFFIC YOU ARE SENDING TO AUTHENTICATION (EG. 3D SECURE) CHANGED?



WHY DID YOU SEND MORE TRANSACTIONS THROUGH AUTHENTICATION?



Over 90% of merchants said that 3DS is important to their fraud strategy. And this is clearly reflected in the percentage of traffic being sent for authentication. On average 65% of merchants across regions say that they're sending more transactions for authentication.

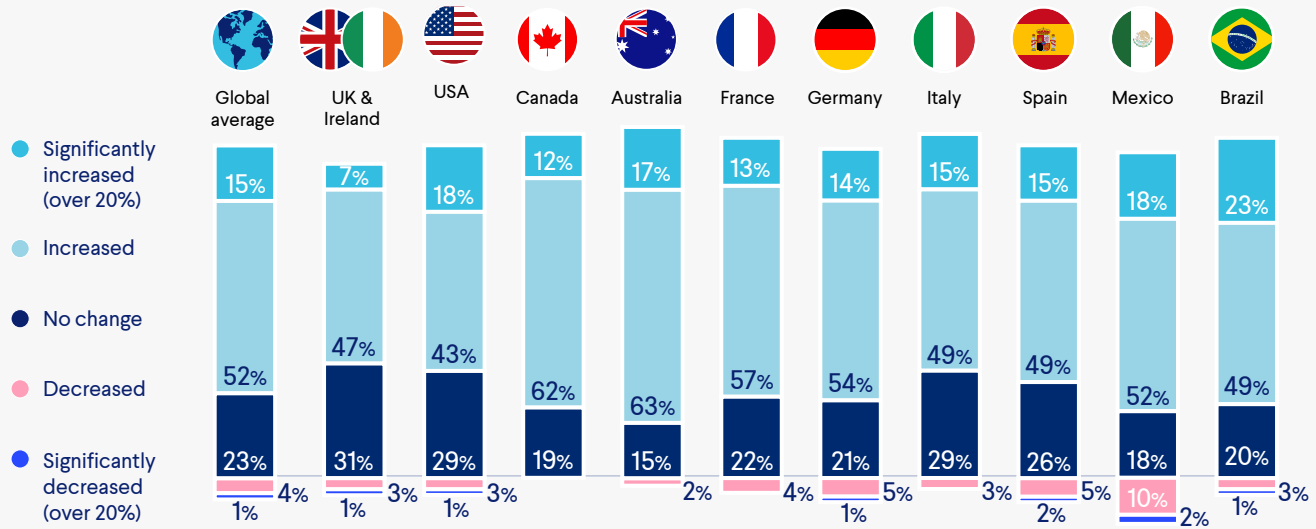
This is much higher for Canadian and Australian merchants. Almost 80% say that they've upped the percentage of transactions they send over the past year. Merchants from these countries point to country regulation and card scheme requirements as the main reasons why.

Over 20% of Brazilian merchants have "significantly" increased their transactions sent to authentication. And almost 40% cite better fraud protection as the reason. A big worry for merchants outside of Europe with the implementation of SCA was that **fraudsters would turn their attention elsewhere.**

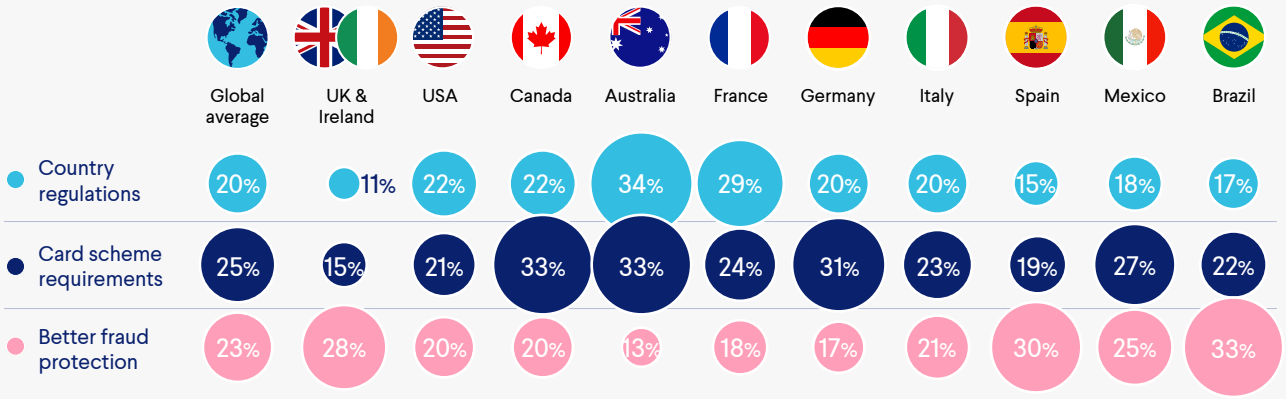
A quarter of merchants across regions report no change. This is particularly true for Spanish and Italian merchants. A third say that the percentage of transactions they're sending have stayed the same. Those that have been sending more transactions mainly chalk this up to wanting better fraud protection.

WILL YOU SEND MORE TRANSACTIONS THROUGH AUTHENTICATION IN 2023?

IN THE NEXT 12 MONTHS, WILL THE AMOUNT OF TRAFFIC YOU SEND TO AUTHENTICATION (EG. 3D SECURE) CHANGE?



WHY DO YOU THINK THAT YOU'LL SEND MORE TRANSACTIONS THROUGH AUTHENTICATION?



On average 67% of merchants across regions see this number going up. And, similar to above, the reasoning behind this varies by country.

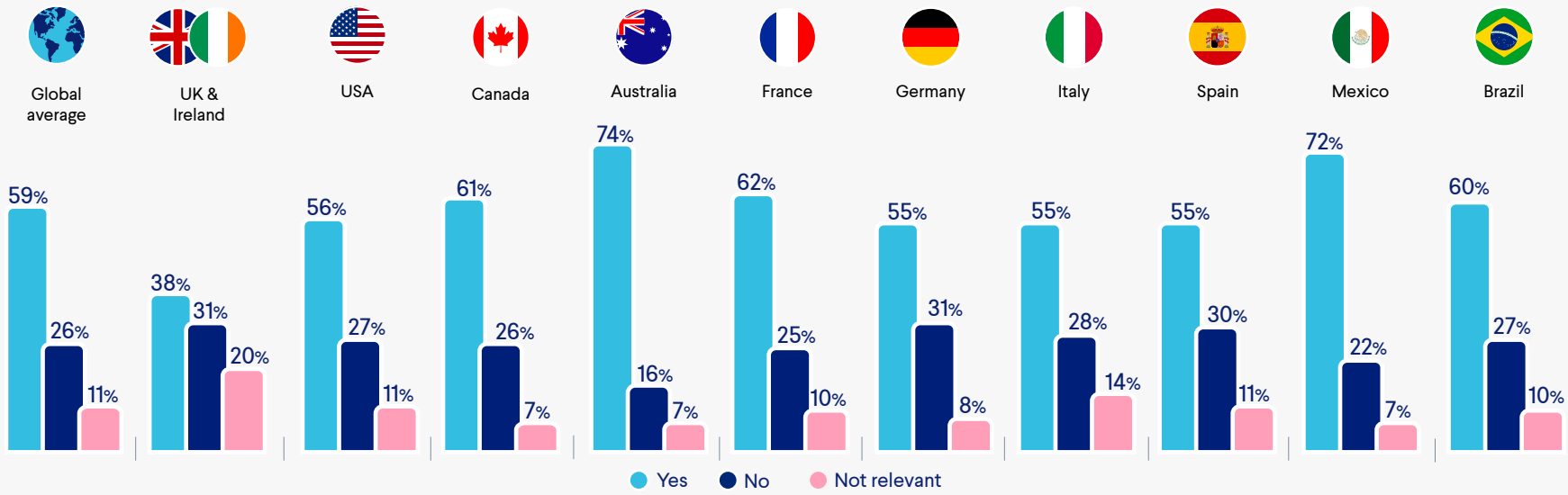
Australian merchants are most likely to predict an increase in transactions sent at almost 80%. And they generally attribute this to country regulation and card schemes. **Australian Payment Network's CNP Fraud Mitigation Framework** only requires SCA for merchants identified as high-risk. But it looks like merchants are taking a "better safe than sorry" approach.

Around a quarter of Brazilian merchants reckon that the percentage of transactions that they're sending for authentication will "significantly" increase. At 33%, they are the most likely to say that this is for better fraud prevention. Sales growth in this region is expected to continue at a **compound annual growth rate (CAGR) of 9.4 percent to 2024**. And increased fraud is bound to follow.

Only 11% of UK and Irish merchants feel that country regulation will influence any increase in the transactions they authenticate. This was below the global average of 20%. Merchants from this region are also the most likely to predict no change to the transactions they send at 31%.

ARE YOU MAKING USE OF SCA EXEMPTIONS?

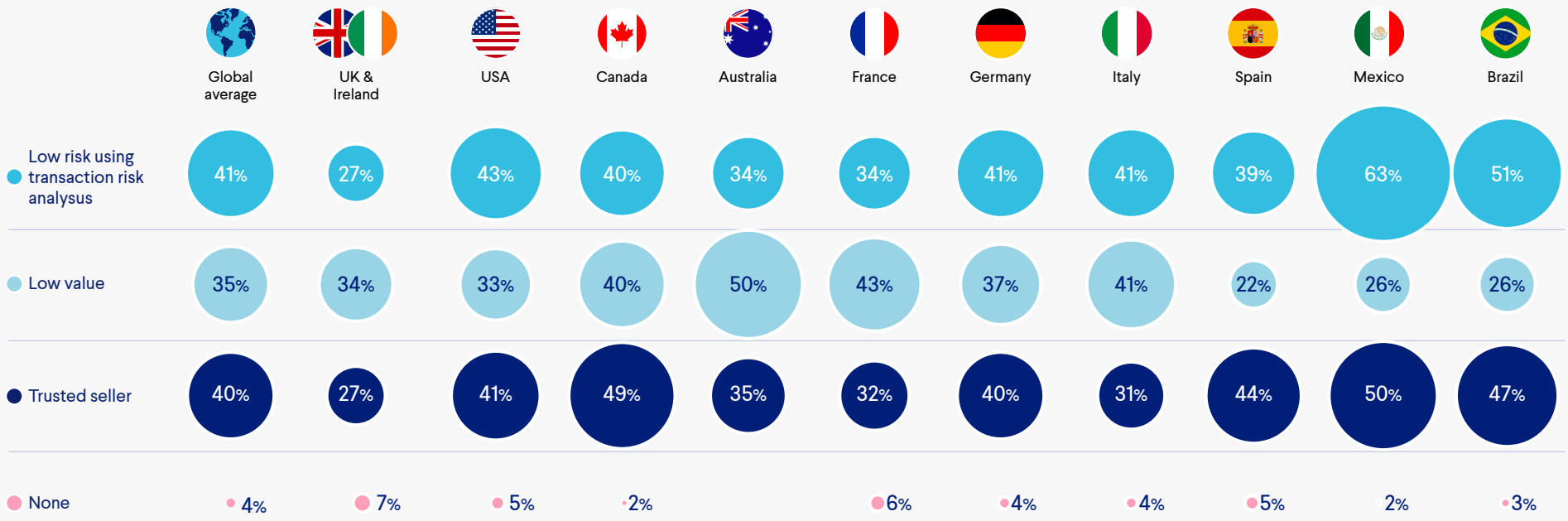
DO YOU CURRENTLY USE EXEMPTIONS AS PART OF YOUR AUTHENTICATION STRATEGY UNDER PSD2?



Getting the most out of exemptions should be the matter of the moment – especially in Europe where PSD2 is mandated. But, on average, only around 50% of European merchants are using exemptions as part of their authentication strategy.

Worryingly, over 10% of European merchants say that exemptions aren't relevant. This is even higher in the UK and Ireland at a massive 20%. Merchants from this region are also the least likely to report using exemptions at under 40%. How many payments could your business be losing to unnecessary 3DS challenges?

WHICH OF THE FOLLOWING EXEMPTIONS DO YOU USE/PLAN TO USE AS A PART OF YOUR PSD2 STRATEGY IN THE FUTURE?



Of the merchants that are using exemptions, which ones are they taking advantage of? If we focus on European merchants, the results are quite evenly split. On average, about 35% of merchants report using each of these exemptions. But this is still lower than we'd expect.

That said, global averages have increased across the board. This is especially true for those using low risk and trusted seller exemptions. Both are up to around 40% from an average of 28% in 2021. So this is promising. Optimizing exemptions is critical to any authentication strategy. You want to protect your customers while offering the most frictionless payment journey.

10.0 COVID-19

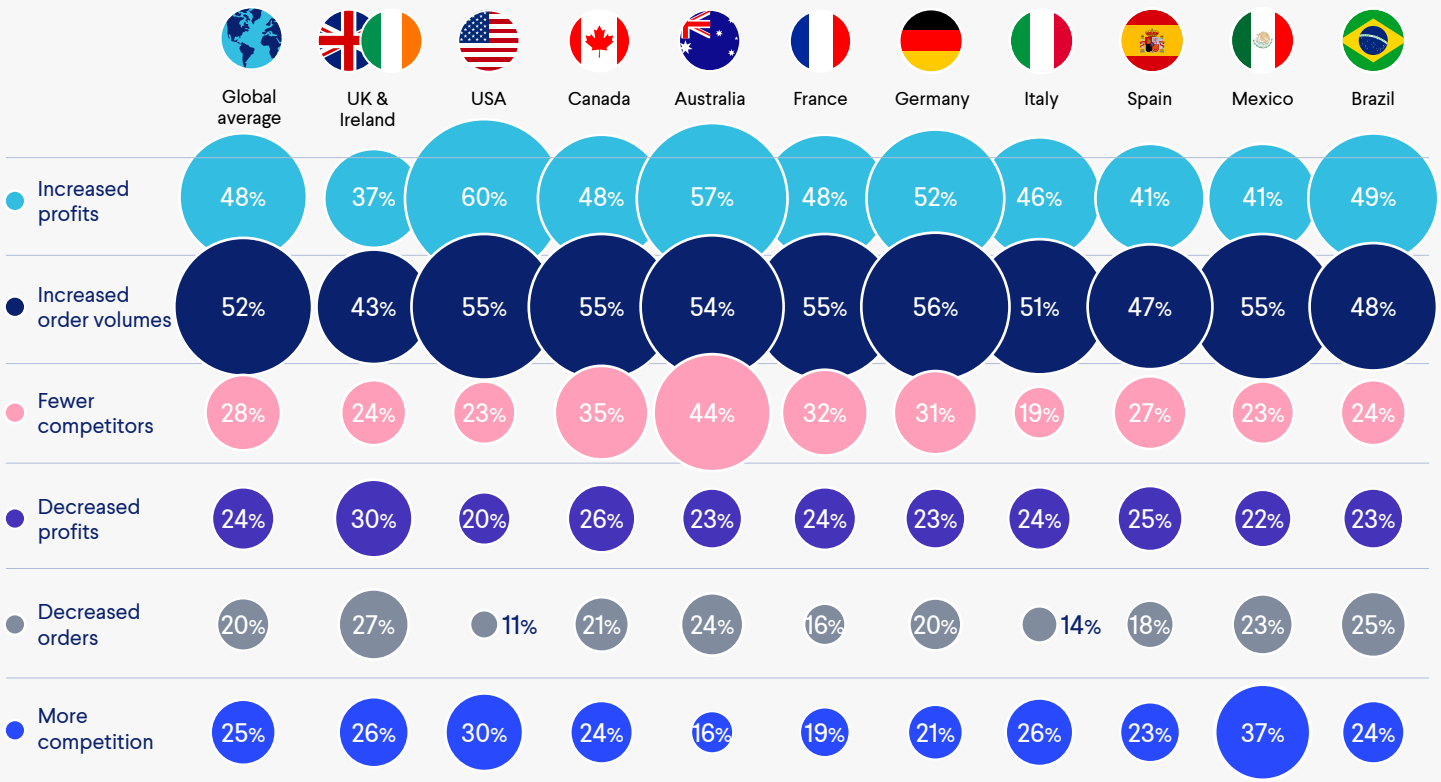
A (hopefully) final reckoning

Travel restrictions and other Covid measures have eased in most parts of the world. And while the term “post-pandemic” might be a little idealized, the dust has probably settled enough that we can assess the long-term impact on ecommerce.

Shops have reopened and the high street is back in full force. But **online shopping is here to stay**. And merchants are **doubling down on consumer-driven commerce**. More specifically, omnichannel, personalization and delivery. But is tackling fraud still high on the agenda?

HOW HAS COVID CHANGED BUSINESS?

WHAT HAS THE LONG-TERM IMPACT OF THE COVID-19 PANDEMIC BEEN ON YOUR FRAUD?

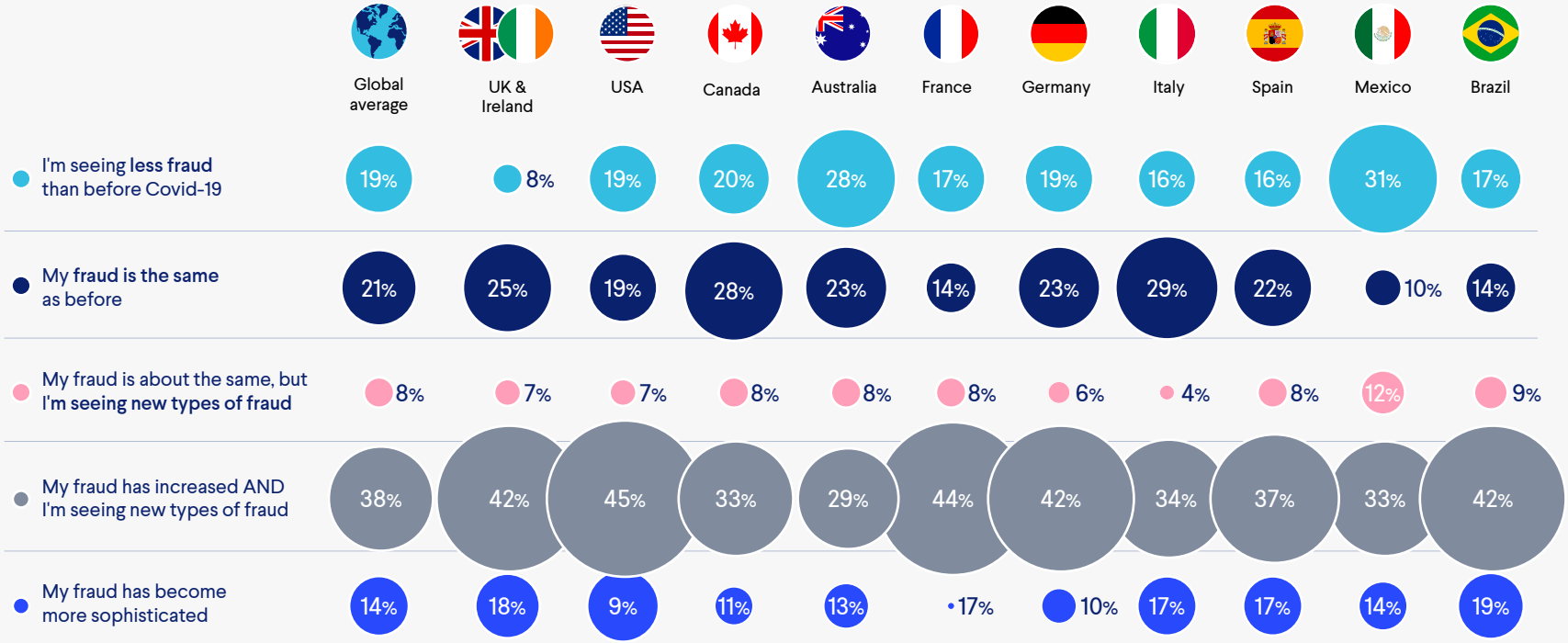


Increased order volumes and profits are the main long-term impacts of the pandemic. Very few report decreased orders. Adopted **pandemic behaviors have become routine** and this includes online shopping. Merchants will need to build an ecosystem that can sustain and support this growth.

US merchants are the most likely to say that profits have increased and the least likely to say that orders have decreased. This view definitely tracks with market data. US online sales exceed $870 billion in 2021. **Reports suggest** that without the sudden consumer shift in response to the pandemic, this wouldn't have been achieved until 2023.

HAS THE PANDEMIC CHANGED YOUR FRAUD?

WHAT HAS THE LONG-TERM IMPACT OF THE COVID-19 PANDEMIC BEEN ON YOUR FRAUD?



How has the pandemic impacted fraud? At best, fraud levels have stayed the same. But a greater proportion of respondents report that fraud levels have increased and that they're seeing new types of fraud. This has shot up to 38% from 20% in 2021.

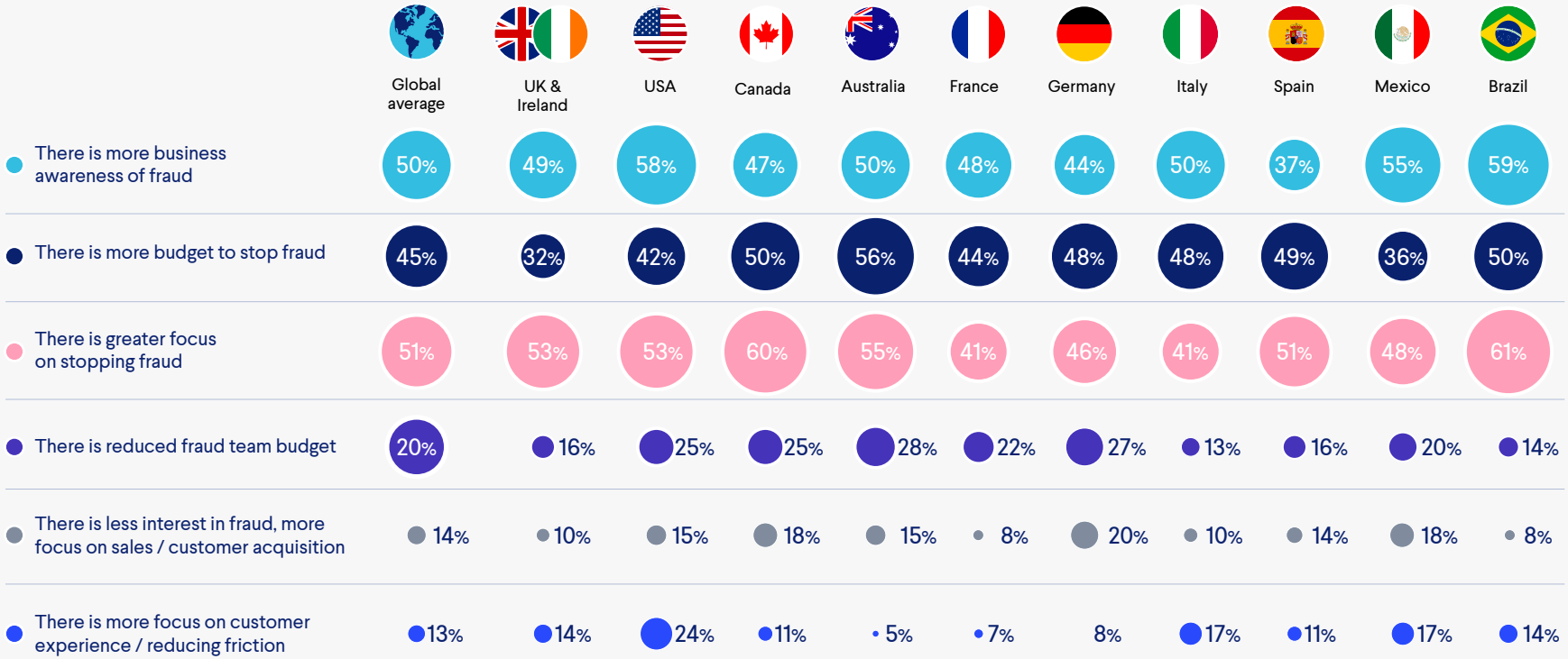
If your business is seeing increased order volumes, you can be sure that fraud is sure to follow. **There is research to suggest** that when traffic increases by 15–20%, you can expect to see a 2–5% increase in fraudulent activity. If you want to continue to thrive in this market, you need robust fraud prevention measures in place.

38%

saw new fraud in 2022 compared to 20% in 2021

HAVE YOUR PRIORITIES CHANGED SINCE THE BEGINNING OF THE PANDEMIC?

HOW HAS THE COVID-19 PANDEMIC IMPACTED YOUR BUSINESS' FRAUD PRIORITIES?



The pandemic has completely transformed the ecommerce market for better and for worse. But how are businesses responding? We wanted to find out how Covid had shifted business priorities...

As expected, the majority of merchants report more awareness of fraud and a greater focus on stopping fraud. And it's great to see in many cases this is backed up with cash – on average 45% of merchants say that there is more budget to stop fraud now.

Globally, there is an emphasis on stopping fraud losses rather than seeing it as an inevitable cost of doing business. Reduced tolerance of fraud by the credit card schemes and issuing banks, as well as a greater emphasis on cost control versus growth, is likely driving this behavior.

11.0 SUMMARY

This survey provides valuable, in-depth understanding into global 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 IMPROVE BUT COLLABORATIONS STALLS

Fraud teams continue to grow in size, but this is starting to slow down in many regions. This is likely in part down to heavier investment in technology and the efficiencies that come with it. The perception and reputation of the fraud team has further improved over the past year. But there's definitely work to do when it comes to cross-departmental collaboration.

2

MERCHANTS USE A VARIETY OF FRAUD TOOLS BUT ARE PRIMARILY RELIANT ON IN-HOUSE SOLUTIONS

Merchants are deploying and seeing success with a range of fraud tools. This is indicative of the dynamic and varied nature of the fraud that they're facing. For the most part, fraud teams report using a mix of in-house and outsourced solutions. But there is still a slight bias towards in-house tools.

3 ONLINE PAYMENT FRAUD AND ACCOUNT TAKEOVER REMAIN TOP FRAUD THREATS, BUT OPPORTUNISTIC FRAUD IS ON THE RISE

There has been a rise in fraud across all types. And merchants globally are seeing an influx of "newer" fraud types. Traditional fraud types continue to be the biggest risk to online merchants, but opportunistic fraud is not too far behind. Refund/returns abuse appears to be the fastest growing fraud threat after online payment fraud.

4 A QUARTER MERCHANTS BELIEVE THAT OVER 10% OF REFUND/RETURNS ARE FRAUDULENT

Policy abuse is quickly becoming a leading fraud threat as the cost of living goes up. And losses have snowballed the issue into a a multi-million dollar problem. On average almost 10% of merchants say that over 20% of returns are the result of abuse, but this could be an underestimation.

5 OVER HALF OF MERCHANTS SAY THEY LOSE UP TO $5 MILLION A YEAR TO ACCOUNT TAKEOVER

Although the reported losses to account takeover are not insignificant, merchants may be overlooking the longer-term financial impact. Merchants are understandably most concerned about revenue loss and the fines associated with data theft. But the negative publicity and operation costs of account recovery have huge financial implications that may not be immediately obvious.

6 MERCHANTS STRUGGLING TO DISPUTE CHARGEBACKS ON NEWER PAYMENT METHODS

Merchants are less likely to win challenges on wallet payments over traditional payment types. This is likely due to a lack of familiarity and difficulty gathering the evidence needed to successfully build a case.

7 3DS IS BECOMING INCREASINGLY MORE RELEVANT OUTSIDE OF EUROPE

The majority of merchants globally consider 3DS "important" or "very important" to their fraud prevention strategy. Adoption outside of mandated regions is likely being spurred on by improvements to the protocol. That said, almost a quarter say that they're "very concerned" about the impact of 3DS on conversion.

Thank you for reading our global fraud trends survey

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

Learn more about Ravelin's fraud and payments services at

ravelin.com