Ravelin

GLOBAL FRAUD TRENDS 2026

FRAUD & PAYMENTS SURVEY REPORT



ravelin.com

CONTENTS

3 DEMOGRAPHICS

4 INTRODUCTION

5 EXECUTIVE SUMMARY

8 SECTION A
THE CONSEQUENCES OF FRAUD

18 SECTION B
CURRENT & EMERGING FRAUD TRENDS

36 SECTION C
FIGHTING FRAUD

45 SECTION D
THE FUTURE OF FRAUD

51 SECTION E
FINDINGS & FRAUDSCAPE ANALYSIS
BY RAVELIN'S CO-FOUNDERS

58 METHODOLOGY

DEMOGRAPHICS



10 countries



4 industries

- ONLINE RETAIL
- TRAVEL, TRANSPORT & HOSPITALITY
- DIGITAL GOODS & SUBSCRIPTIONS
- ONLINE MARKETPLACES

86%
sell both online and in stores

14%
only sell online

INTRODUCTION

Welcome to the **sixth edition of Ravelin's annual report** on global ecommerce fraud trends.

We surveyed 1504 professionals working in key positions within the Fraud, Payments, C-level and related teams, for enterprise-level ecommerce companies in ten countries from across the globe.

We focused our research on four key sectors of the digital economy: Online Retail; Travel, Transport & Hospitality; Digital Goods & Subscriptions; Online Marketplaces.

In this report's 60 pages, you'll explore merchants' **observations, takeaways and predictions** about the fraud and abuse they face, AI's relationship to fraud and risk, consumer and merchant behaviors, anti-fraud strategies, and much more.

Crucially, where relevant, we also show you how findings compare to previous years, how different countries responded, and where corporate functions and teams had different opinions and attitudes.

Our goal? **To enhance your understanding of the fraudscape** as it stands today and as it's transforming into the future – and ultimately **to help you manage threats and take advantage of opportunities**.

We hope you find our data and insights illuminating and useful.

Team Ravelin

EXECUTIVE SUMMARY

Key takeaways and insights from Ravelin's Global Fraud Trends 2026 – Fraud & Payments Survey Report at a glance.



01. The line between customers and criminals is blurring

- Consumer fraud is a growing headache, with **43%** of merchants noticing a rise in fraudulent behavior from first parties.
- Merchants are now evenly split on **whether professional criminals or abusive first parties pose the biggest threat** to their business.
- As the market looks toward the expansion of autonomous agentic commerce, AI is seen as more trustworthy than humans by 53%, further confirming this erosion of transactional trust in the human consumer.



02. Fraudsters are adopting AI faster than businesses

- Artificial intelligence is drastically altering the fraud landscape. Bad actors are aggressively weaponizing AI, with **67% of merchants receiving AI-generated fake refund evidence**.
- The financial impact is tangible, as most organizations attribute 5 to 15% of their fraud losses to AI-supported attacks.
- At the same time, defensive capabilities are lagging behind; **30% of enterprises do not use anti-fraud AI** or machine learning.
- 1 in 3 respondents identified AI as the single biggest fraud challenge their company will face in the next year.

03. Fraud volumes are potentially stabilizing – but most struggle to quantify

- Most merchants (**66%**) report increased fraud volumes in the past year. However, the rate of growth has decelerated, dropping by 11% compared to the previous period.
- Looking forward, just over half (52%) of merchants expect fraud to continue to increase, and **78%** predict their spending to combat fraud will increase.
- At the same time, over half say they struggle to quantify the scale of refund abuse, indicating that **certain types of fraud might go underreported**.

04. Fraud costs continue to climb despite maturing controls

- While responses indicate that rapid spikes in fraud volumes may be stabilizing, the financial drain continues to compound. The average annual loss per enterprise in 2026 **reached $11.4 million**, marking a 7.5% year-over-year escalation.
- More than 2 in 5 enterprises **lose 1%+ of their revenue** to fraud and abuse.
- Financial loss is becoming more important, with **48%** of businesses identifying lost revenue as their top consequence of fraud – a 9% year-on-year increase.

05. The friction paradox is a primary barrier to mitigation

- A clear disconnect exists between recognizing the problem and implementing the solution. Although **66%** of organizations acknowledge they need to be doing more to combat fraud, internal systemic bottlenecks often paralyze decisive action.
- The obstacles are **not primarily budgetary** (cited by only 22%), but rather an institutional fear that tighter security may introduce transaction friction and damage the brand's public image – with the two most frequently **cited as an obstacle**.
- Merchants' preference lies firmly with **dynamic friction** – yet merchants clearly favor stricter prevention (43%) over maximizing payment acceptance no matter the cost (8%).

06. Unchecked fraud degrades loyalty and market valuation

- Paradoxically, although friction is perceived as a top obstacle to implementing stronger detection, 81% **say that customers don't trust companies perceived to have weak fraud defenses**, while 77% agree that publicized fraud incidents directly erode customer loyalty.
- The potential impact is significant, considering **one in three** companies report receiving **negative publicity** in the past year as a result of fraud attacks.
- The fallout of compromised security reaches further, as **64%** of enterprises report experiencing a direct drop in their stock price following media coverage linking their brand to fraud – a sometimes overlooked consequence.

Make sure you read our Co-Founders' analysis of the survey results on page 51.

SECTION A

THE CONSEQUENCES OF FRAUD

The first section of our annual Fraud Trends Report is always dedicated to the consequences of fraud.

From the reported costs of fraud to eroding customer loyalty and even stock price hits, fraud and abuse have wide consequences in ecommerce.

Explore our findings to make better strategic decisions and support your company's growth.

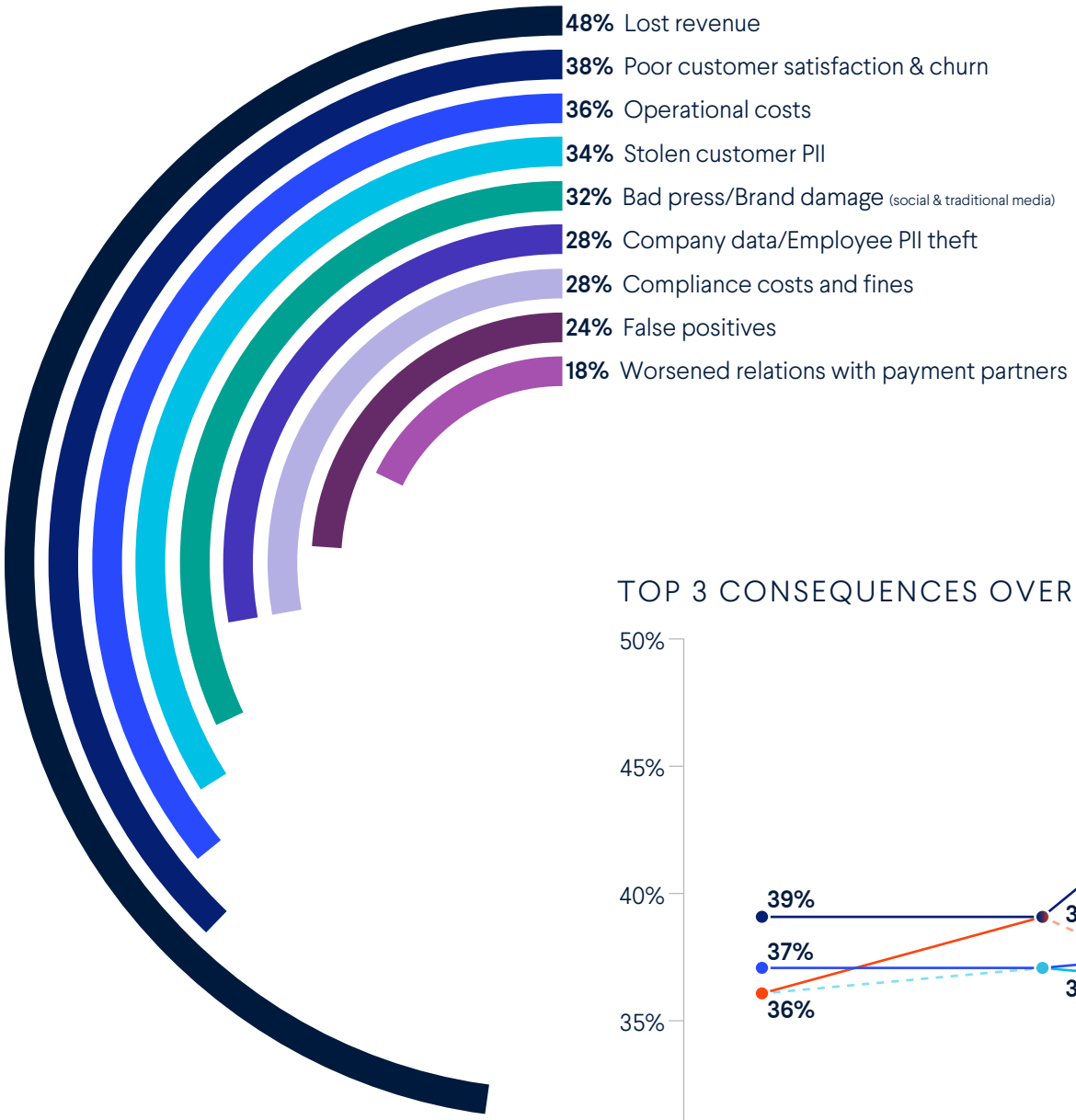
KEY FINDINGS

48%
report financial losses to fraud

$11.4m
average loss per enterprise

78%
are worried about fraud

CONSEQUENCES OF FRAUD



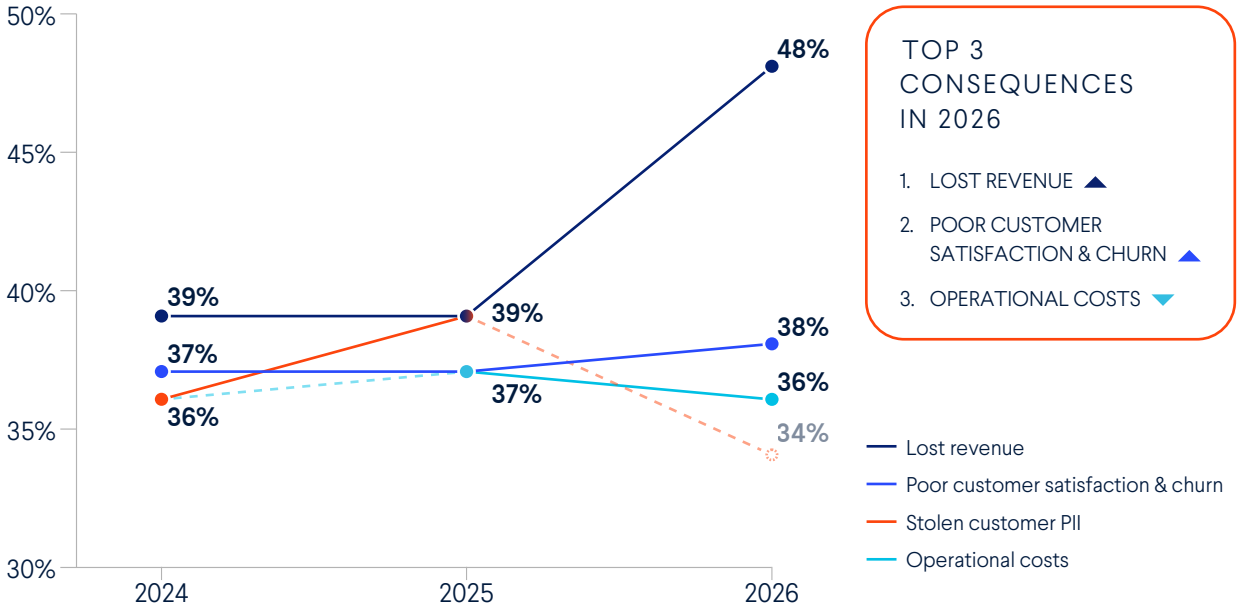
"Which of these potential consequences of fraud have affected your company in the past 12 months? Choose all that apply"

COSTS & CUSTOMER LOSS THE BIGGEST PAIN POINTS

Fraud may be quantifiable in many cases, but it's not just about cold hard numbers. Fraud teams may have good reason to scrutinize block rates and chargeback rates, yet it helps to remember that the consequences of fraud are diverse and wide-reaching.

With **fraud damaging public perception, causing customer churn and skyrocketing operational costs**, the message is clear: Fraud prevention ought to be everyone's business, not just one team's. But it's often up to fraud managers to spread the word and achieve buy-in. Use this data to your advantage.

TOP 3 CONSEQUENCES OVER TIME



At Ravelin, we know that every company's fraud is different. And **even within the same sector, no two companies have the exact same fraudscape, despite certain similarities in fraudsters' tactics and methods**.

While detection should never be a one-size-fits-all approach, it helps to also remember the top consequences of fraud for our four key ecommerce sectors surveyed.

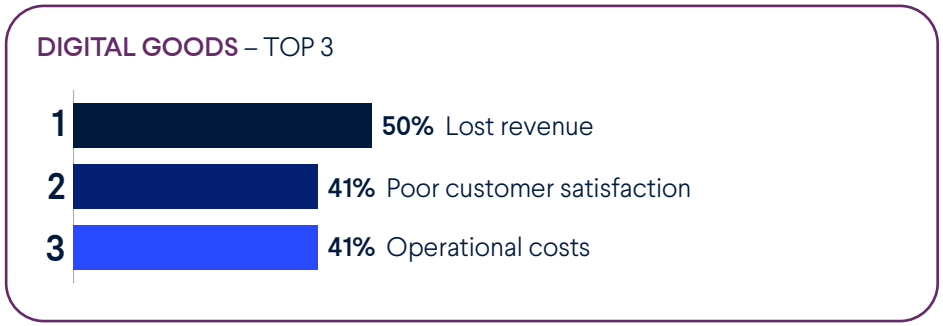
This year sees the continuation of a focus on costs and financial concerns, which we first saw in 2025. Travel is the only sector where lost revenue did not rank at the very top of the table of fraud consequences – but that's little consolation, as it remains only one percentile lower, in number 2.

With tightening budgets, operational costs continue to be in the spotlight. Perhaps cross-team communication can help alleviate some of these pains.

As for customer satisfaction, it's almost the other side of the same coin. Disgruntled customers churn – sometimes abandoning their cart, others just not returning.



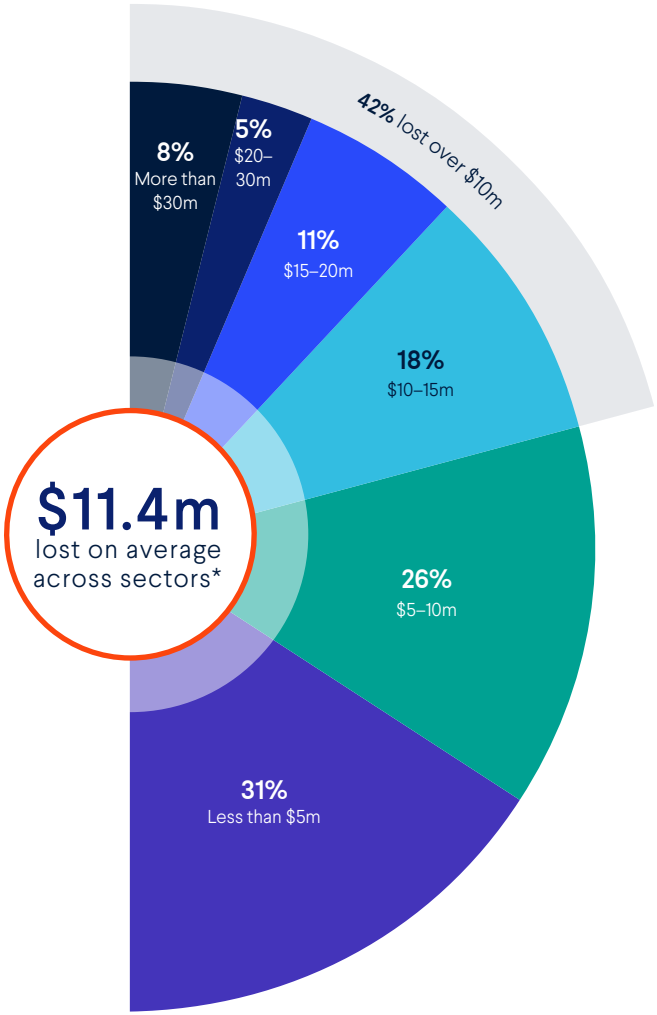






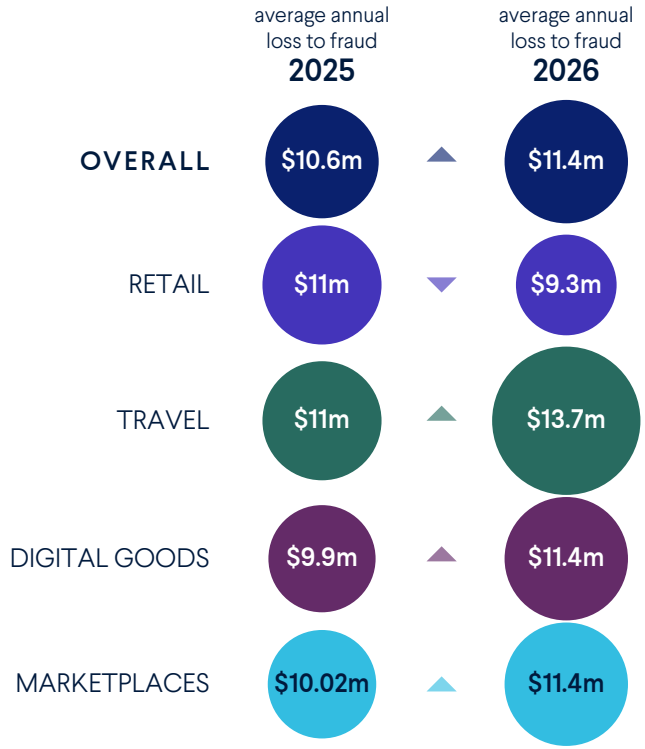
THE COST OF FRAUD IS ON THE RISE

SELF-REPORTED ANNUAL COST OF FRAUD



"How much does fraud cost your company per year (in USD)?"

Y-O-Y CHANGES TO THE COST OF FRAUD



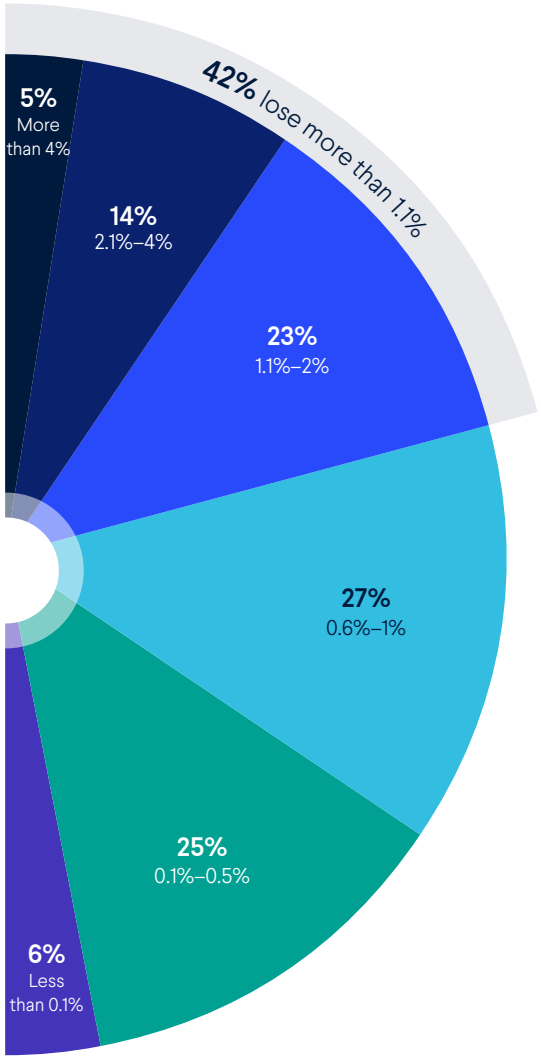
It's good news for the Retail industry, as reported fraud costs have slightly decreased in the past year. Yet **across the board, an enterprise loses $11.4 million to fraud every year**, which represents a modest albeit unwelcome +7.5% year-on-year increase. For more than 4 in 10 companies, the average loss to fraud is bigger than $10m a year.

Travel and Digital Goods have been in fraudsters' crosshairs, owing to the characteristics of these two sectors. Near-zero-click and immediate fulfillment have won over consumers, but provide unique opportunities to fraudsters as well.

*Estimated averages based on the midpoint of each range, and $40m used for "More than $30m"

MERCHANTS LOSE >1% OF REVENUE TO FRAUD – CNP AND REFUND ABUSE THE COSTLIEST

% OF REVENUE LOST TO FRAUD

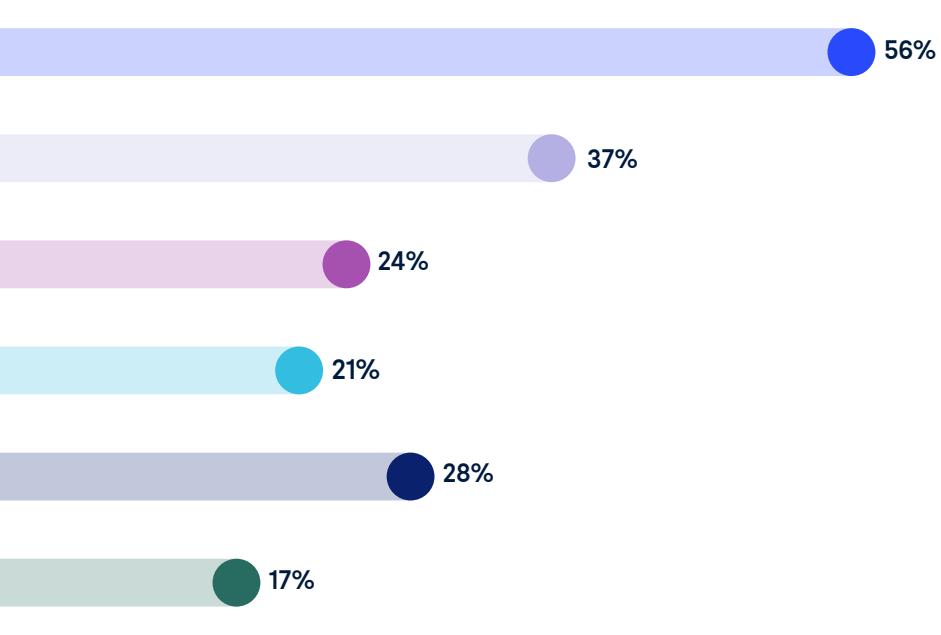


"Approximately what percentage of your annual revenue is lost to fraud?"

Participating merchants were asked about their two most costly fraud types, as well as share how much fraud eats into their revenue. The results show **persistent losses to payment fraud**, with more than half selecting it as their costliest type. The **devastating consequences of first-party fraud** were also highlighted in their answers, with chargeback fraud ranking in second place, and refund abuse in third across sectors.

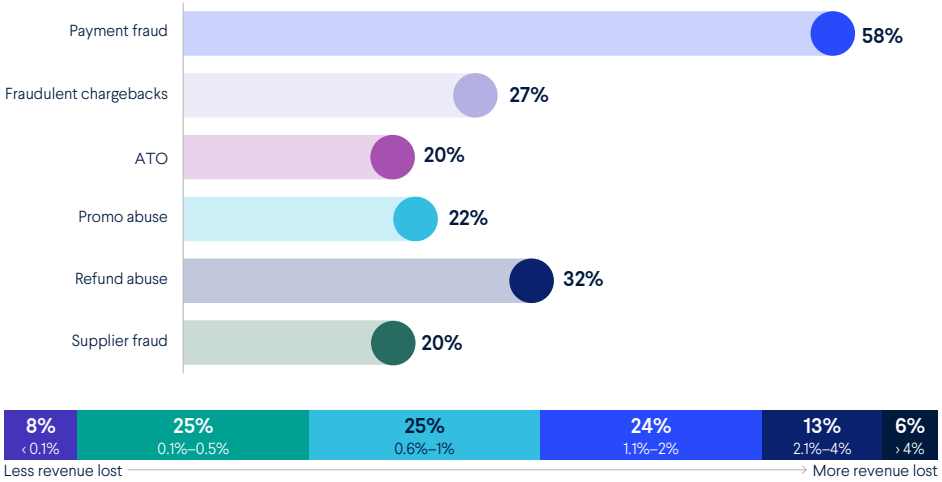
For more than **4 in 10 merchants, fraud and associated abuse brought losses of over 1% of their revenue**. Considering we spoke to enterprise merchants exclusively, these sums are sizeable.

MOST EXPENSIVE FRAUD TYPES

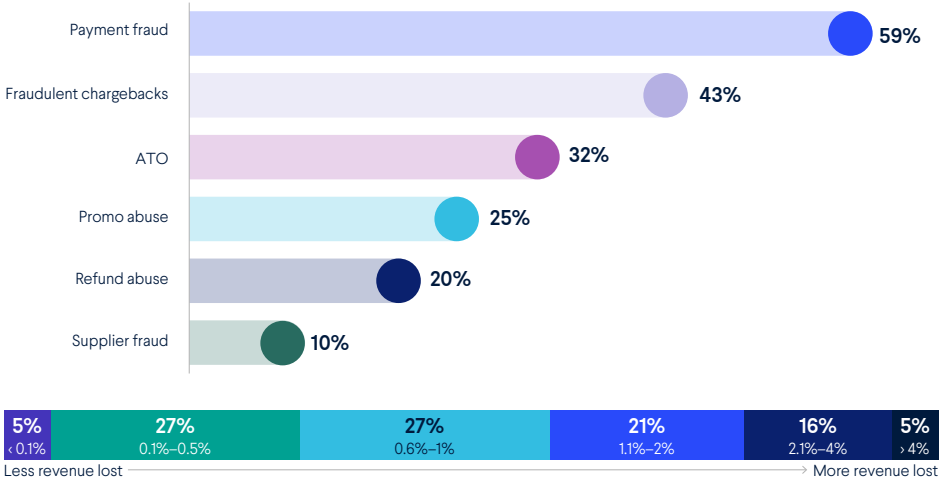


"Of the following, which types of fraud and abuse cost your business the most? Select up to 2."

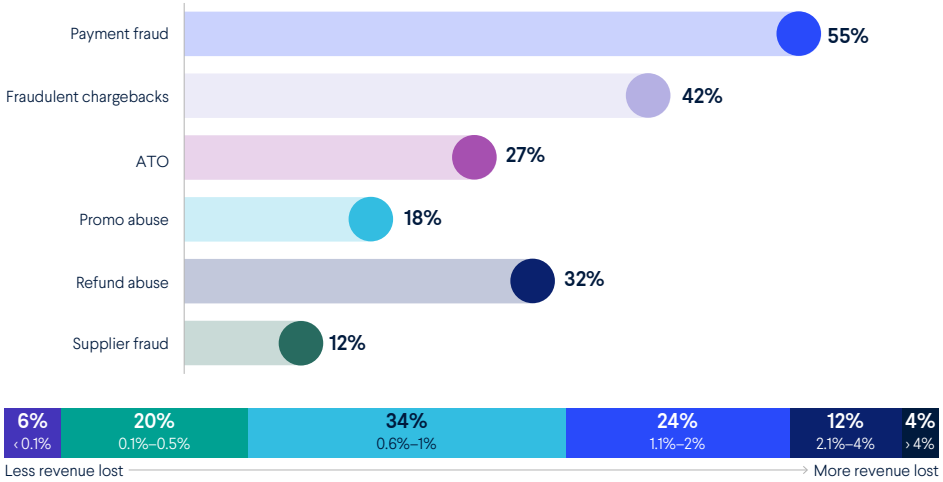
RETAIL – COSTLIEST FRAUD TYPES & REVENUE LOSS TO FRAUD



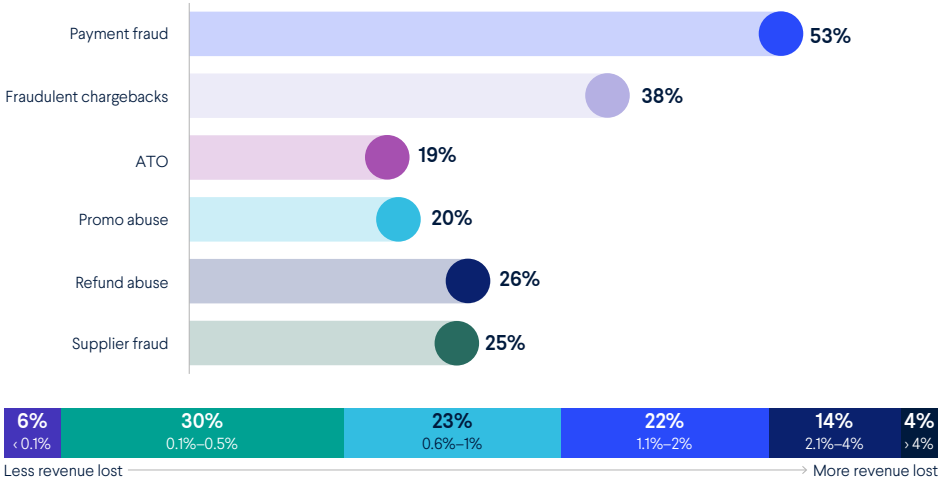
TRAVEL – COSTLIEST FRAUD TYPES & REVENUE LOSS TO FRAUD



DIGITAL GOODS – COSTLIEST FRAUD TYPES & REVENUE LOSS TO FRAUD



ONLINE MARKETPLACES – COSTLIEST FRAUD TYPES & REVENUE LOSS TO FRAUD



Looking deeper at sector-specific results, different pain points have been plaguing different industries. **Marketplaces**, for instance, have more seller fraud. This is to be expected. However, we also saw prominent refund abuse in **Digital Goods** – where returns are obviously not feasible, refunds can be more complicated.

Travel is plagued by account takeover attacks, with motivators including the theft of miles and similar valuable credit. Fraudulent chargebacks are expensive for both Digital Goods and Travel, with merchants attempting to navigate a perhaps more complex regulatory framework than elsewhere, along with protecting their bottom lines.

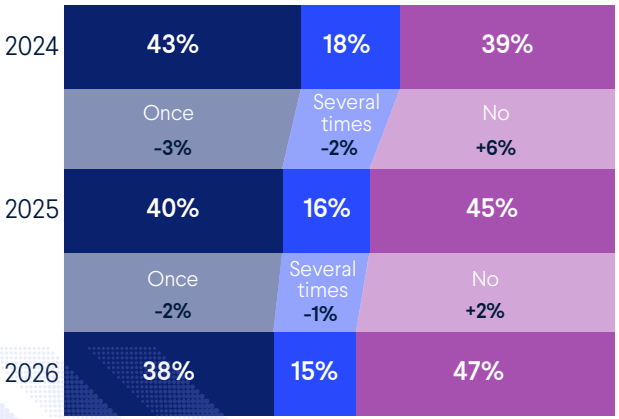
MEDIA COVERAGE IS UNDERMINING CUSTOMER LOYALTY

Public perception and opinion is an important area of focus in our survey, as merchants' experiences can shed more light on the link between fraud and consumer loyalty.

For one more year, most merchants saw mentions of their brand in relation to fraud either in traditional or social media, though this percentage slightly decreased by 2% in 2026.

But what do these mentions mean for merchants? Roughly eight in ten agree that publicity around fraud erodes loyalty and trust.

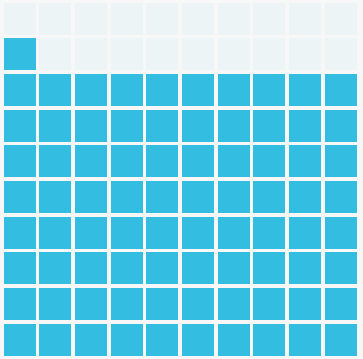
COMPANIES LINKED TO FRAUD IN THE NEWS



"In the past 12 months, has your company been featured in the press or social media as a result of fraud?"

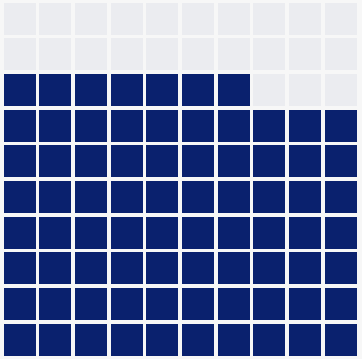
MERCHANT OPINIONS ON FRAUD AND PUBLIC IMAGE

"Customers **don't trust companies** perceived to have weak fraud protection."



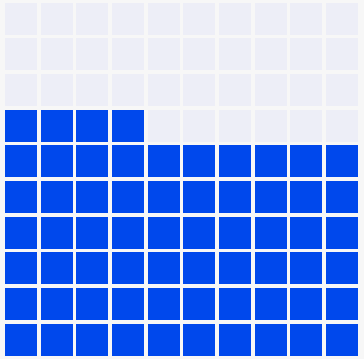
81% agree

"When customers see reports of fraud against our company or customers, **they become less loyal** to us."



77% agree

"Media or social media reports of fraud/abuse against our company have **caused our stock price to drop**."



64% agree

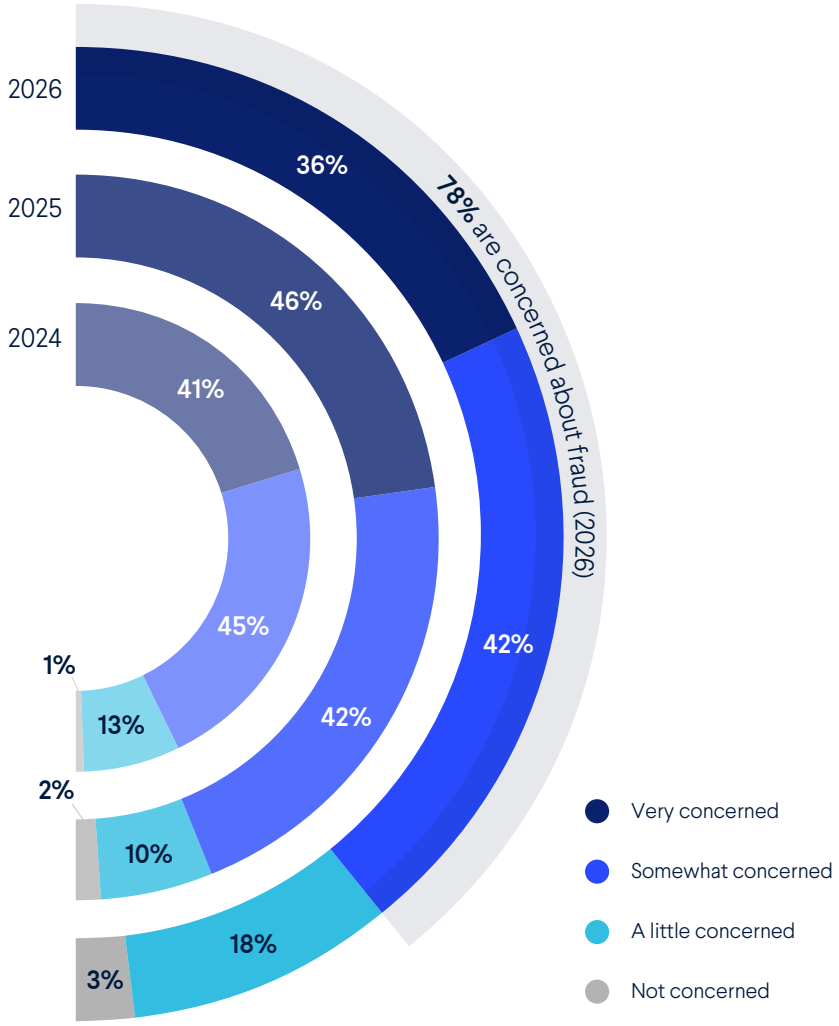
This domino effect goes even further though, with 64% having experienced drops in stock prices as a result of fraud-related publicity online and/or offline.

To build trust, merchants can showcase their strong fraud defenses through public campaigns or case studies.

> **"Your customers care that your online shop is safe from fraud – use your robust fraud strategy to instill confidence."**
>
> Martin Sweeney, CEO at Ravelin

FRAUD WORRIES ARE HIGH – BUT DECLINING

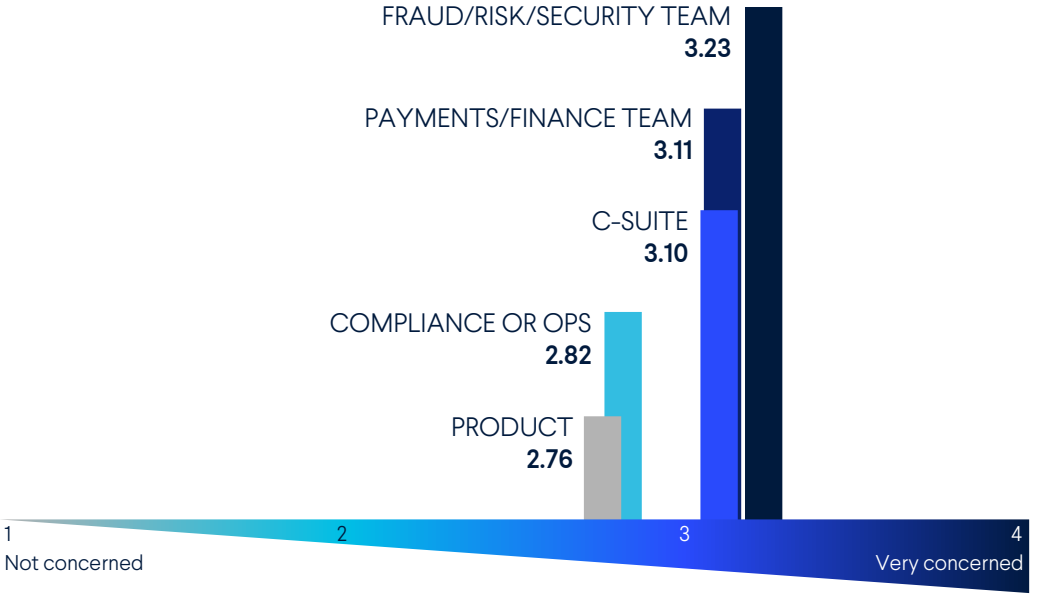
LEVEL OF MERCHANT CONCERN ABOUT THE VOLUME OF FRAUD



"How concerned are you about the volume of fraud faced by your company at present?"

78%
are concerned about fraud

AVERAGE CONCERN LEVEL BY ROLE

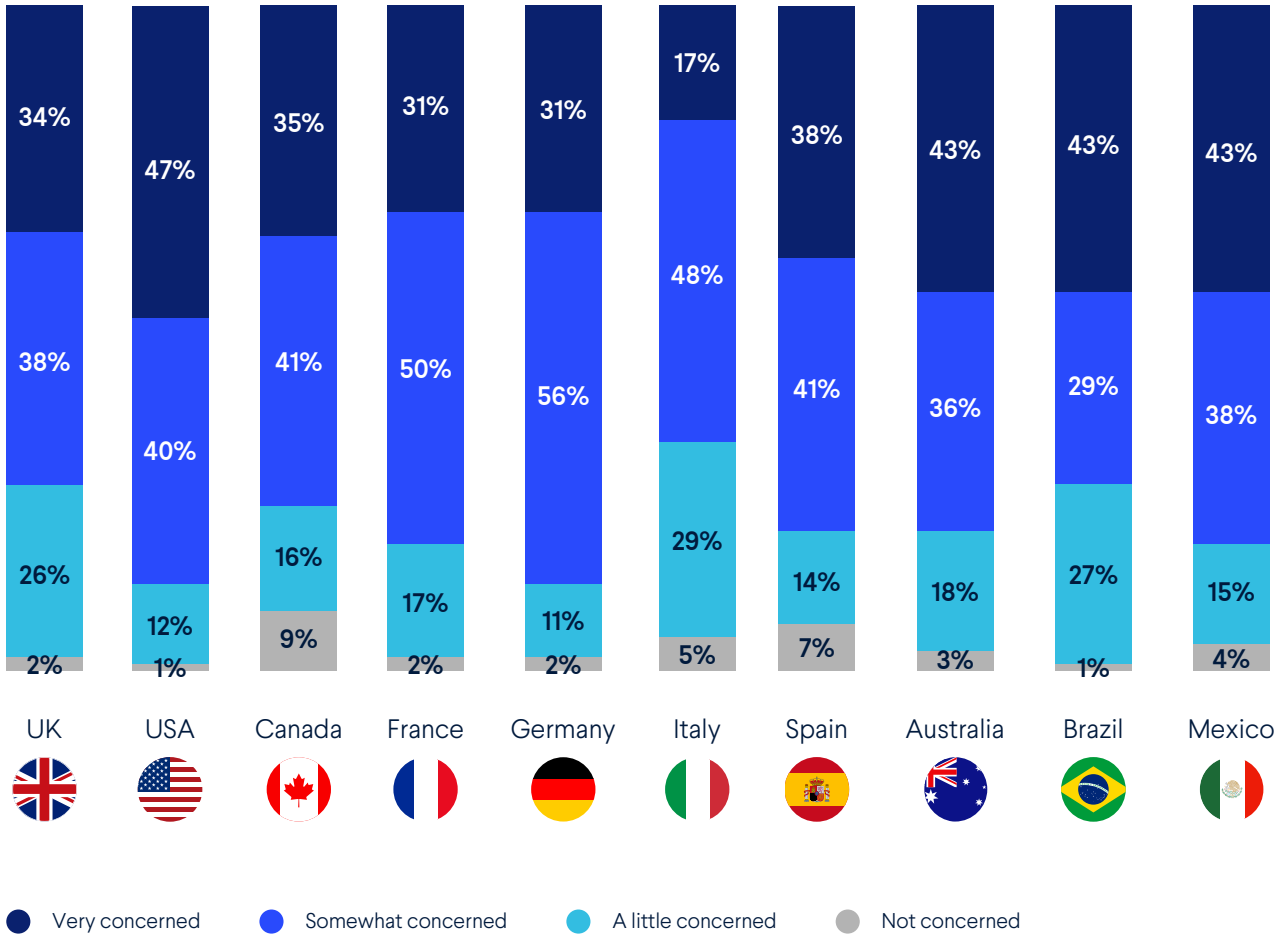


Weighted position based on cohort responses on a scale of 1 (not concerned) to 4 (very concerned).

"We saw slightly lower levels of acute concern this year – possibly reflecting more mature controls and better-prepared teams. But take heed: Fraud and abuse remain significant."

Mairtin O'Riada, COO at Ravelin

LEVEL OF MERCHANT CONCERN ABOUT THE VOLUME OF FRAUD – COUNTRY-SPECIFIC



Survey results examined separately for each of our ten countries demonstrate a high degree of variation.

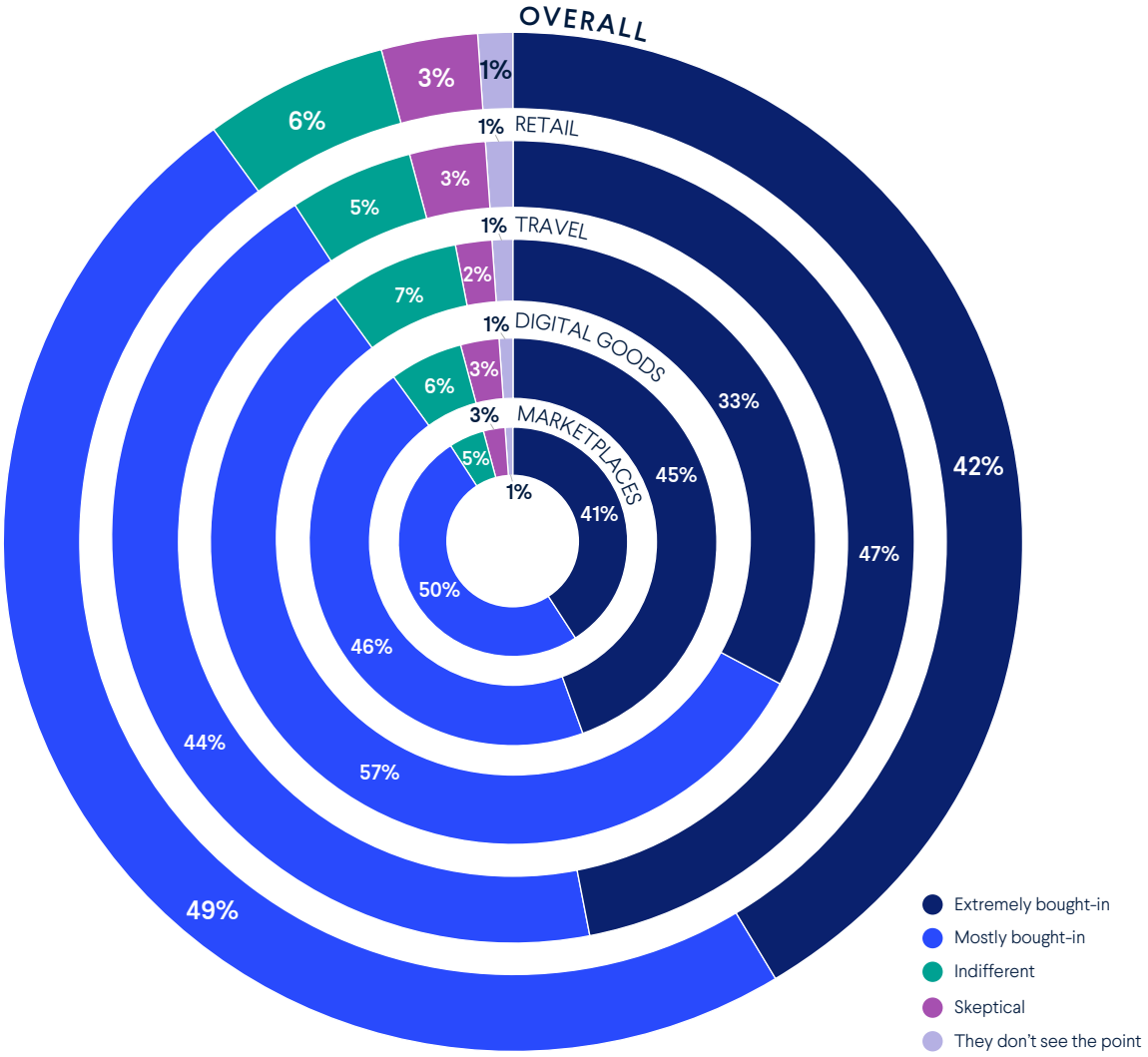
The USA and Germany are the most concerned about fraud, at a combined 87% each.

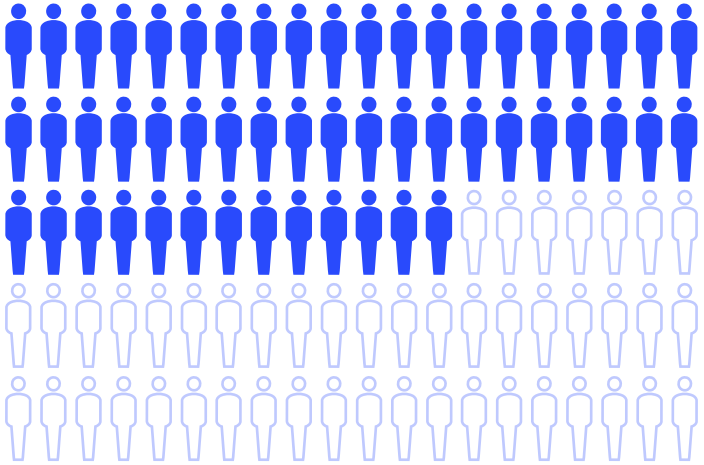
On the other side of the spectrum are Italy (34% little or no concern) as well as **the UK and Brazil** with 28% expressing little or no concern in each country.

Lower levels of concern may reflect more mature controls, better-prepared fraud teams, and **growing familiarity with operating in a high-fraud environment**, even as other forms of abuse remain significant.

SENIOR LEADERS REGARD FRAUD AS A KEY ISSUE

C-SUITE BUY-IN ON THE IMPORTANCE OF STOPPING FRAUD & ABUSE





53% of leaders
see fraud as a "cost of doing business" that cannot be meaningfully reduced

"How bought-in are leaders/C-suites at your company on the importance of stopping fraud and/or abuse? (If you're a leader, please reply about your fellow leaders at your company)"

SECTION B

CURRENT & EMERGING FRAUD TRENDS

This second section is all about the fraud trends that merchants from across the spectrum of ecommerce have observed in the past year.

We set out to discover quantitative and qualitative changes in fraud and abuse, including first-party fraud trends, how AI is weaponized against companies by bad actors, chargeback trends, and refund trends.

How does your fraud compare to your peers?

KEY FINDINGS

66%

report a rise in fraud, which is an improvement on previous years

Payments & refunds

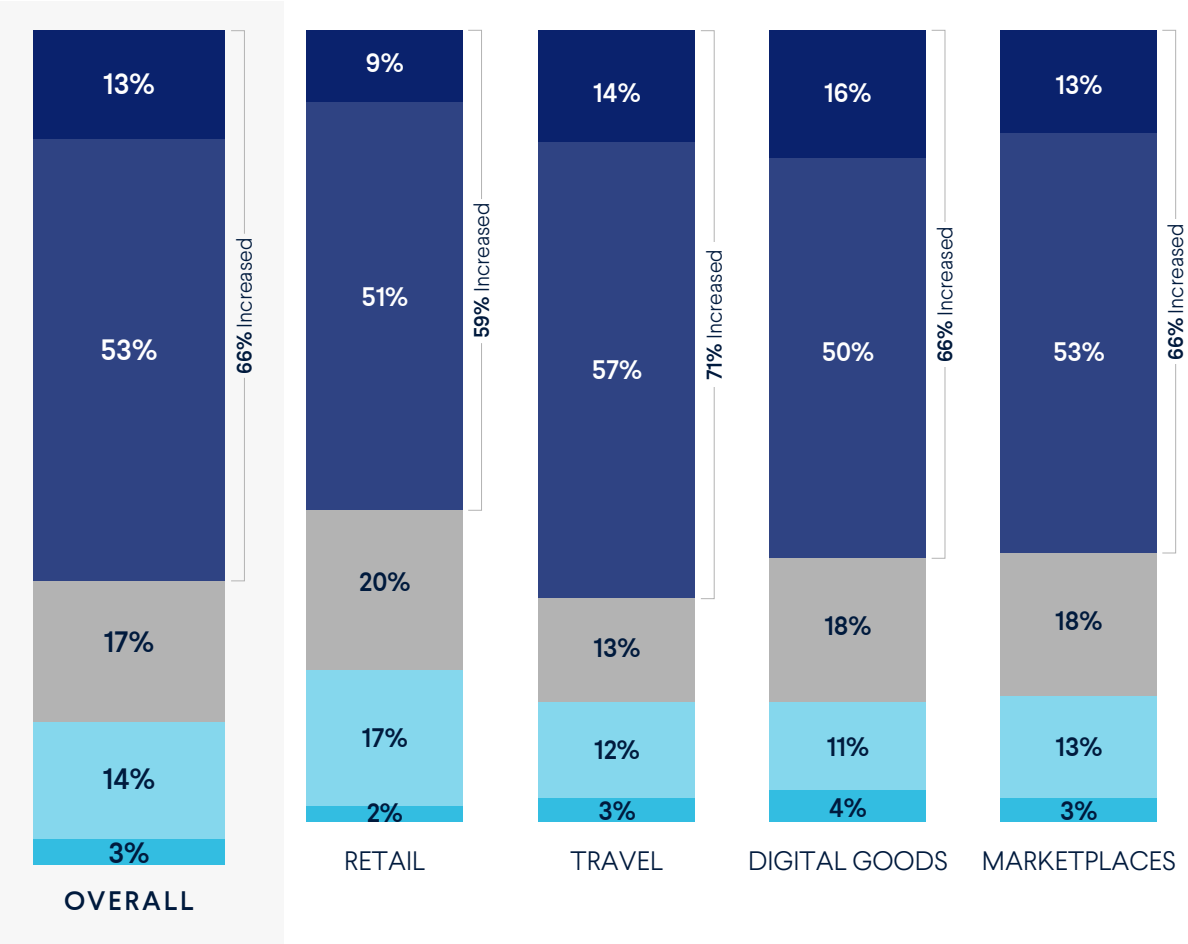
most affected by fraud in 2026

67%

have received AI-generated fake refund evidence

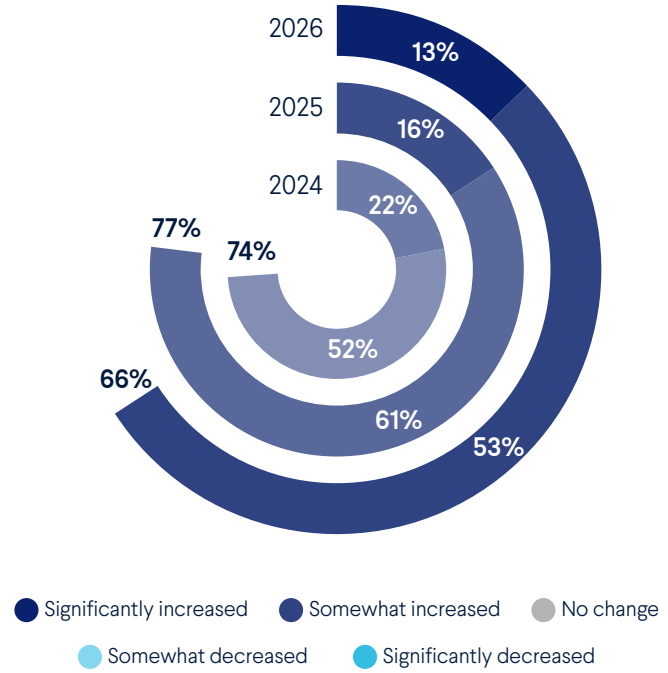
FRAUD CONTINUES TO RISE – BUT THERE ARE GOOD SIGNS

YEAR-ON-YEAR CHANGE TO FRAUD RATES



"In the past 12 months, have you noticed a change in the volume of fraud that affects your company?"

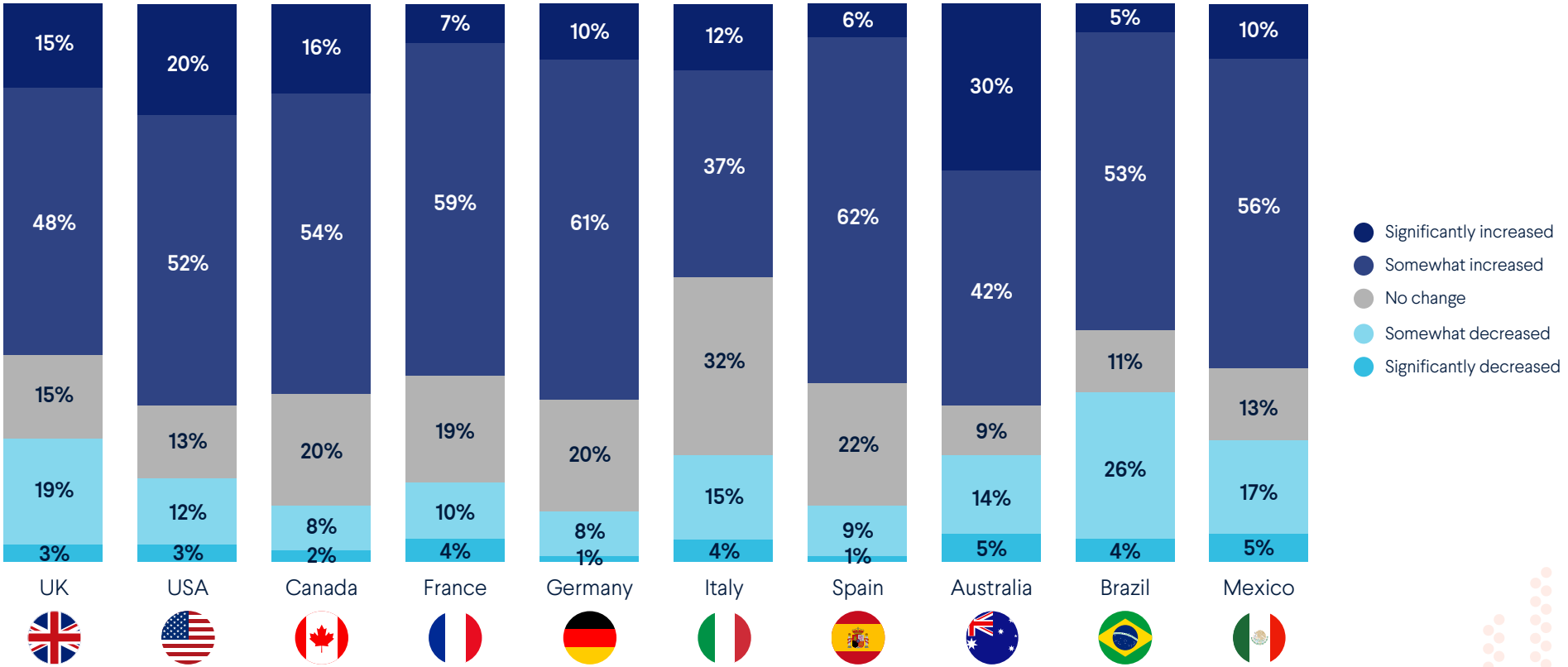
FRAUD INCREASE BY YEAR



Considered together with previous years, 2026 results suggest that fraud is **becoming more contained and manageable** for many merchants, with more reporting stability or modest decline rather than sharp increases.

This could be reflective of stronger controls, greater operational maturity, and wider use of data-led prevention.

YEAR-ON-YEAR CHANGES TO FRAUD RATES – COUNTRY-SPECIFIC



"In the past 12 months, have you noticed a change in the volume of fraud that affects your company?"

Of the survey's 10 countries, **Australia and the USA have emerged as the primary fraud hotspots**, with 72% of merchants in both countries reporting increased fraud.

Three in ten Australian merchants saw "significant" increase, which is the highest percentage across the board. Note that "significant" increase was specified as a rise of at least +20%.

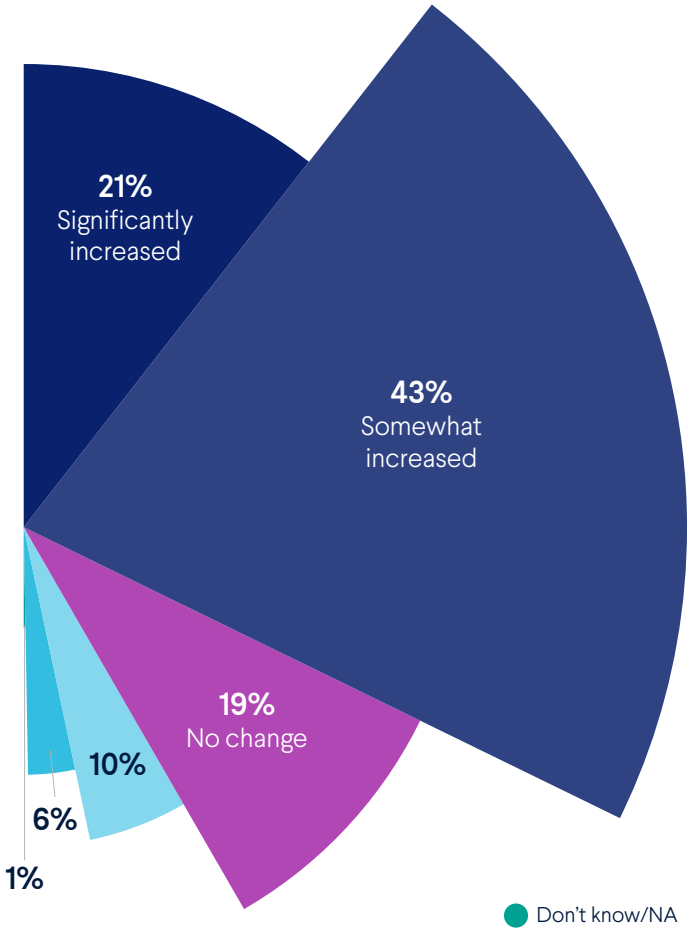
Completing the top four are **Germany and Canada**, with increases for 71% and 70% of businesses respectively..

At the opposite end of the spectrum, **Brazil** emerged as the country with the biggest self-reported drop in fraud, as 30% of Brazilian merchants surveyed said their fraud decreased. It was followed by **the UK and Mexico** – nations which tied at 22% for reported drops in fraud – then Australia and Italy at 19%.

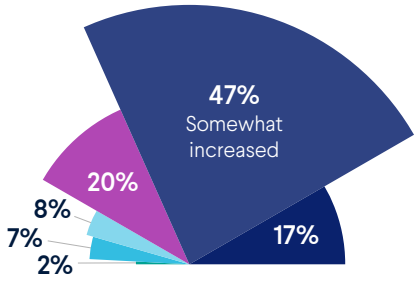
Uniquely, Australia appears on both the list of highest reported increases and highest reported decreases in fraudulent activity. This is because only 9% of Australian merchants said that fraud stayed the same for them.

FRAUD PAIN POINT #1: ONLINE PAYMENT FRAUD (CNP FRAUD) TRENDS

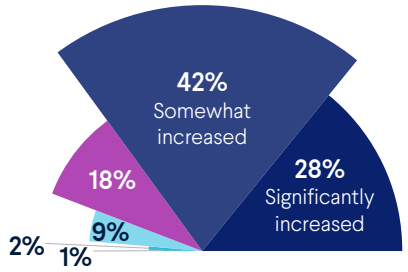
OVERALL



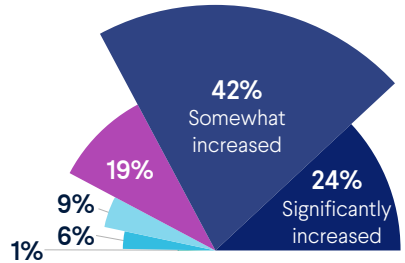
RETAIL



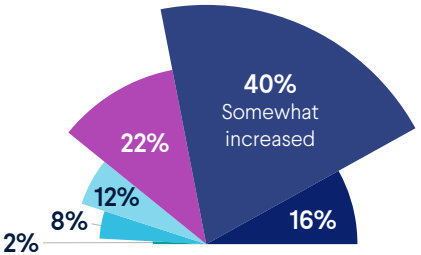
TRAVEL



DIGITAL GOODS



MARKETPLACES

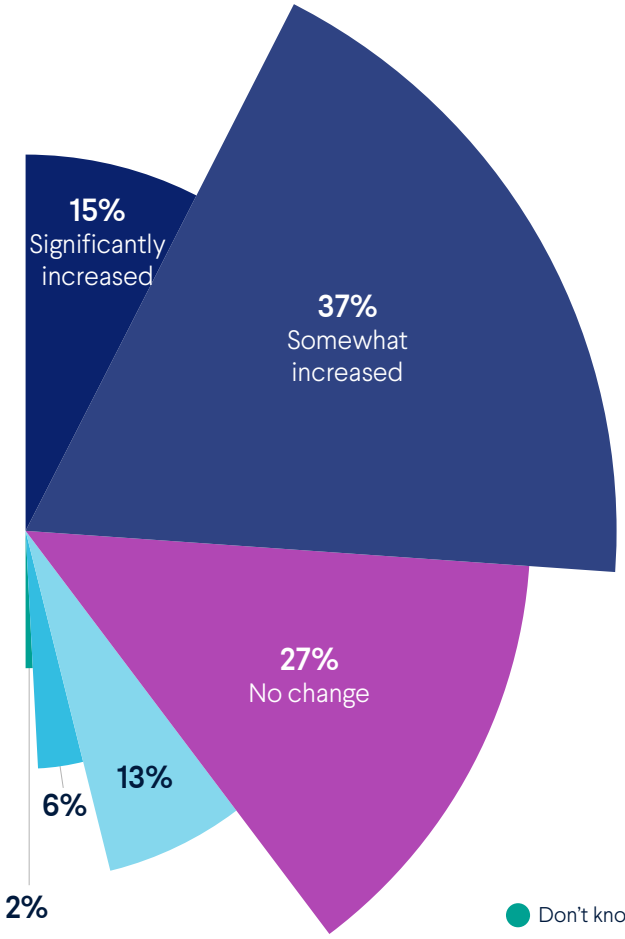


Don't know/NA | Significantly decreased | Somewhat decreased | No change | Somewhat increased | Significantly increased

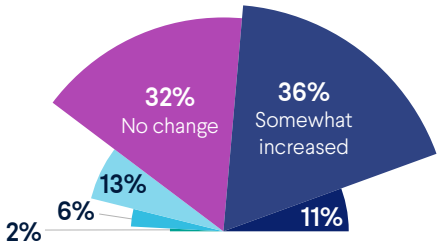
"How has each of these fraud types changed at your company in the past 12 months? Online payment fraud (e.g. stolen cards)"

FRAUD PAIN POINT #2: FRAUDULENT CHARGEBACK (FRIENDLY FRAUD) TRENDS

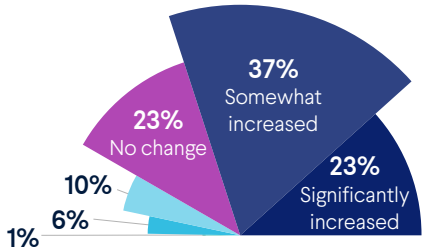
OVERALL



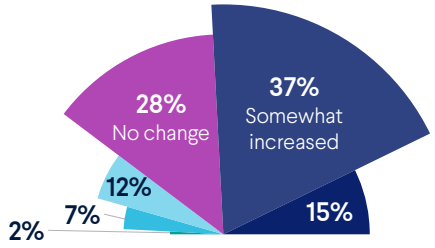
RETAIL



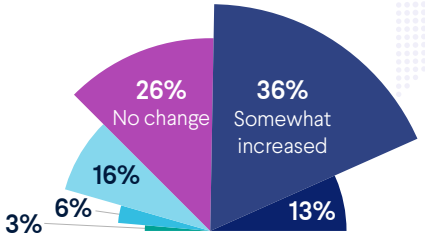
TRAVEL



DIGITAL GOODS



MARKETPLACES

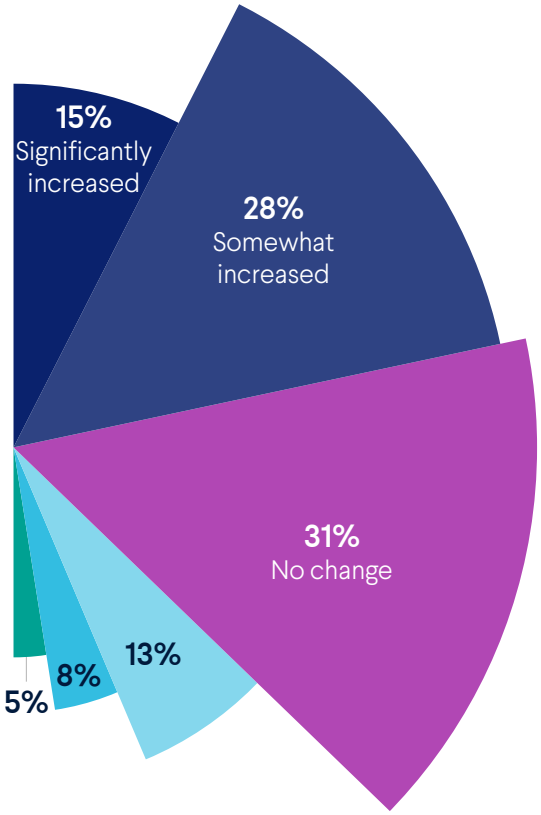


Don't know/NA | Significantly decreased | Somewhat decreased | No change | Somewhat increased | Significantly increased

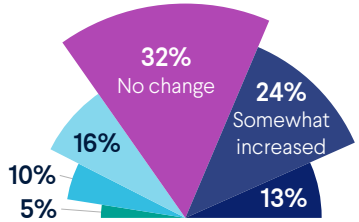
"How has each of these fraud types changed at your company in the past 12 months? Fraudulent chargebacks (friendly fraud)"

FRAUD PAIN POINT #3: ACCOUNT TAKEOVER ATTACKS (ATO) TRENDS

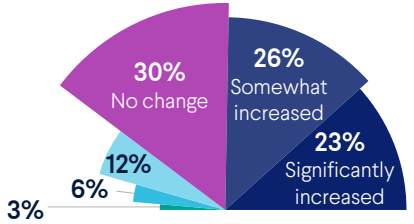
OVERALL



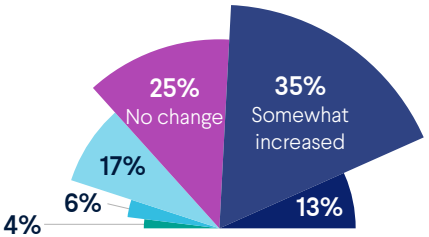
RETAIL



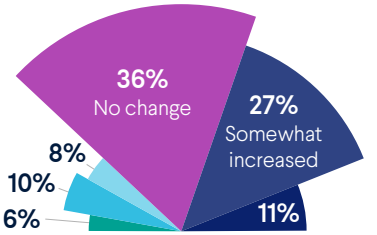
TRAVEL



DIGITAL GOODS



MARKETPLACES

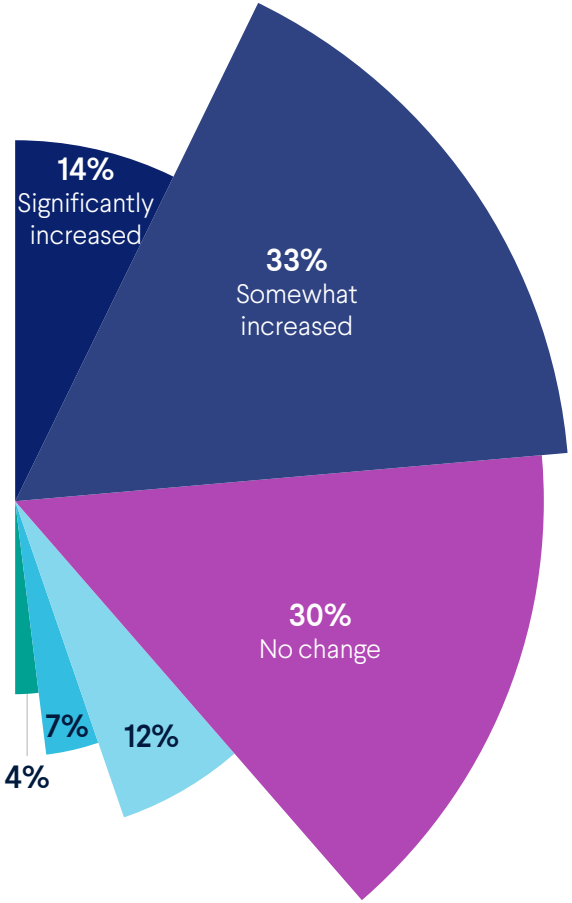


Don't know/NA | Significantly decreased | Somewhat decreased | No change | Somewhat increased | Significantly increased

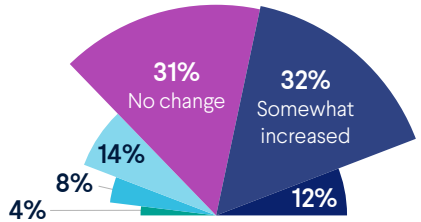
"How has each of these fraud types changed at your company in the past 12 months? Account takeover attacks"

FRAUD PAIN POINT #4: PROMO, VOUCHER & POLICY ABUSE TRENDS

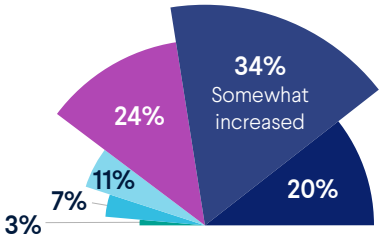
OVERALL



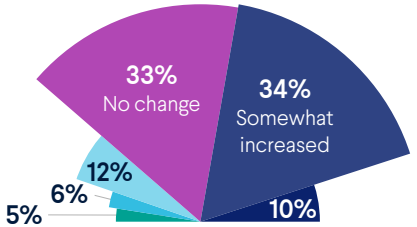
RETAIL



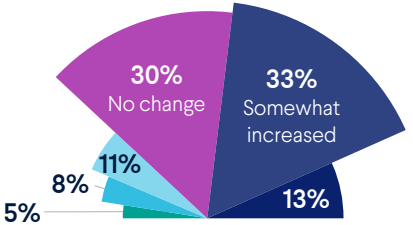
TRAVEL



DIGITAL GOODS



MARKETPLACES

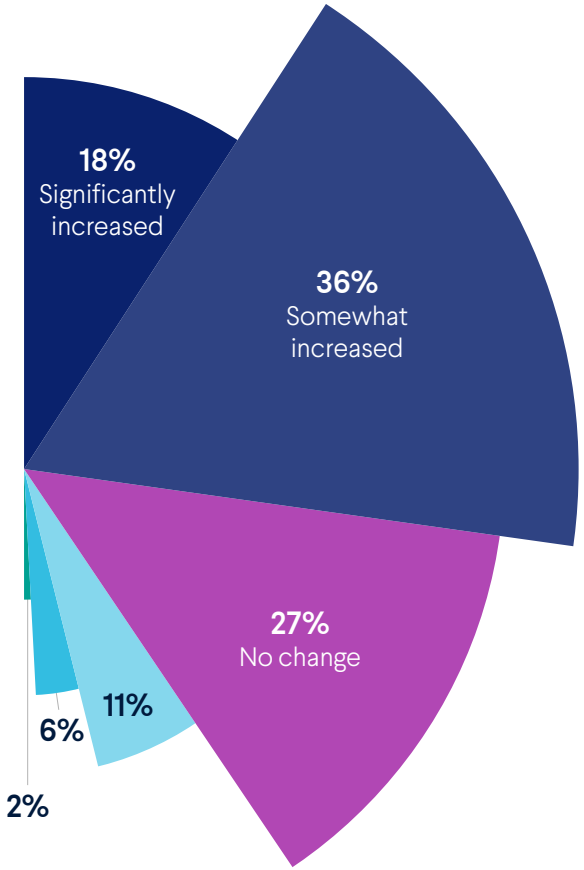


Don't know/NA | Significantly decreased | Somewhat decreased | No change | Somewhat increased | Significantly increased

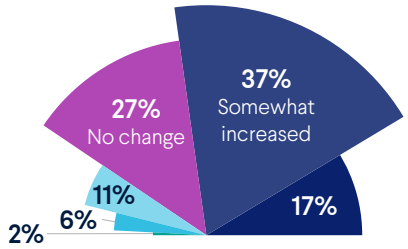
"How has each of these fraud types changed at your company in the past 12 months? Promo, voucher and related policy abuse"

FRAUD PAIN POINT #5: REFUND ABUSE TRENDS

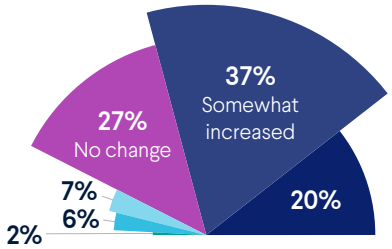
OVERALL



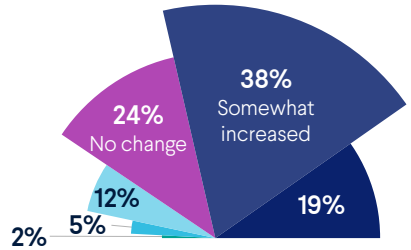
RETAIL



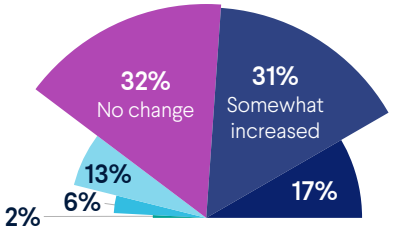
TRAVEL



DIGITAL GOODS



MARKETPLACES

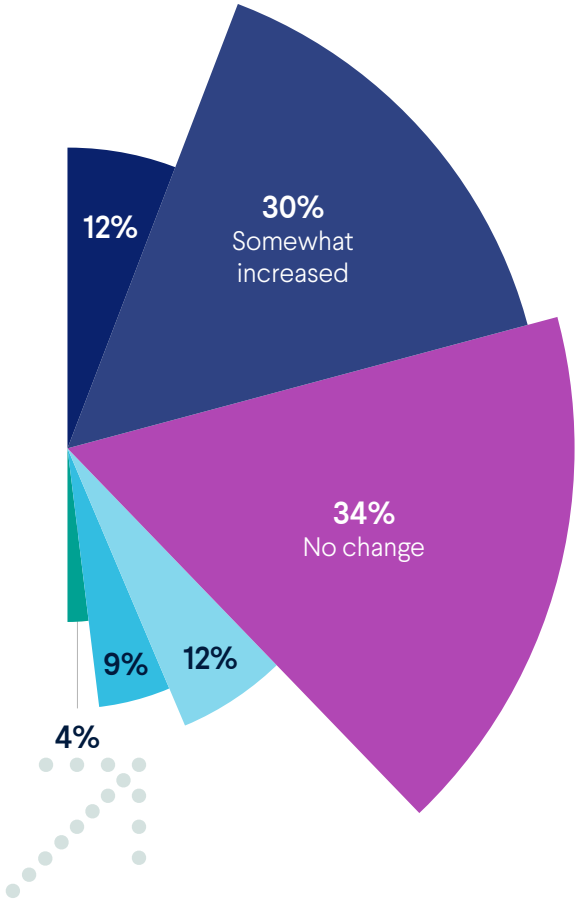


Don't know/NA | Significantly decreased | Somewhat decreased | No change | Somewhat increased | Significantly increased

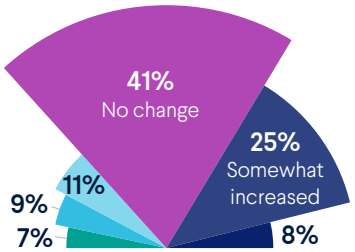
"How has each of these fraud types changed at your company in the past 12 months? Refund abuse"

FRAUD PAIN POINT #6: SUPPLIER, PARTNER & MARKETPLACE SELLER FRAUD TRENDS

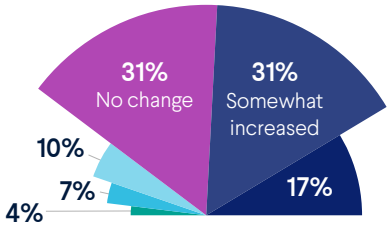
OVERALL



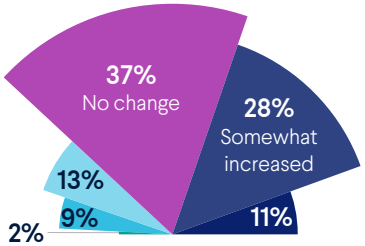
RETAIL



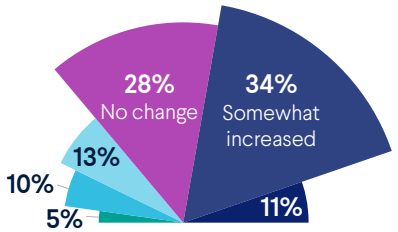
TRAVEL



DIGITAL GOODS



MARKETPLACES

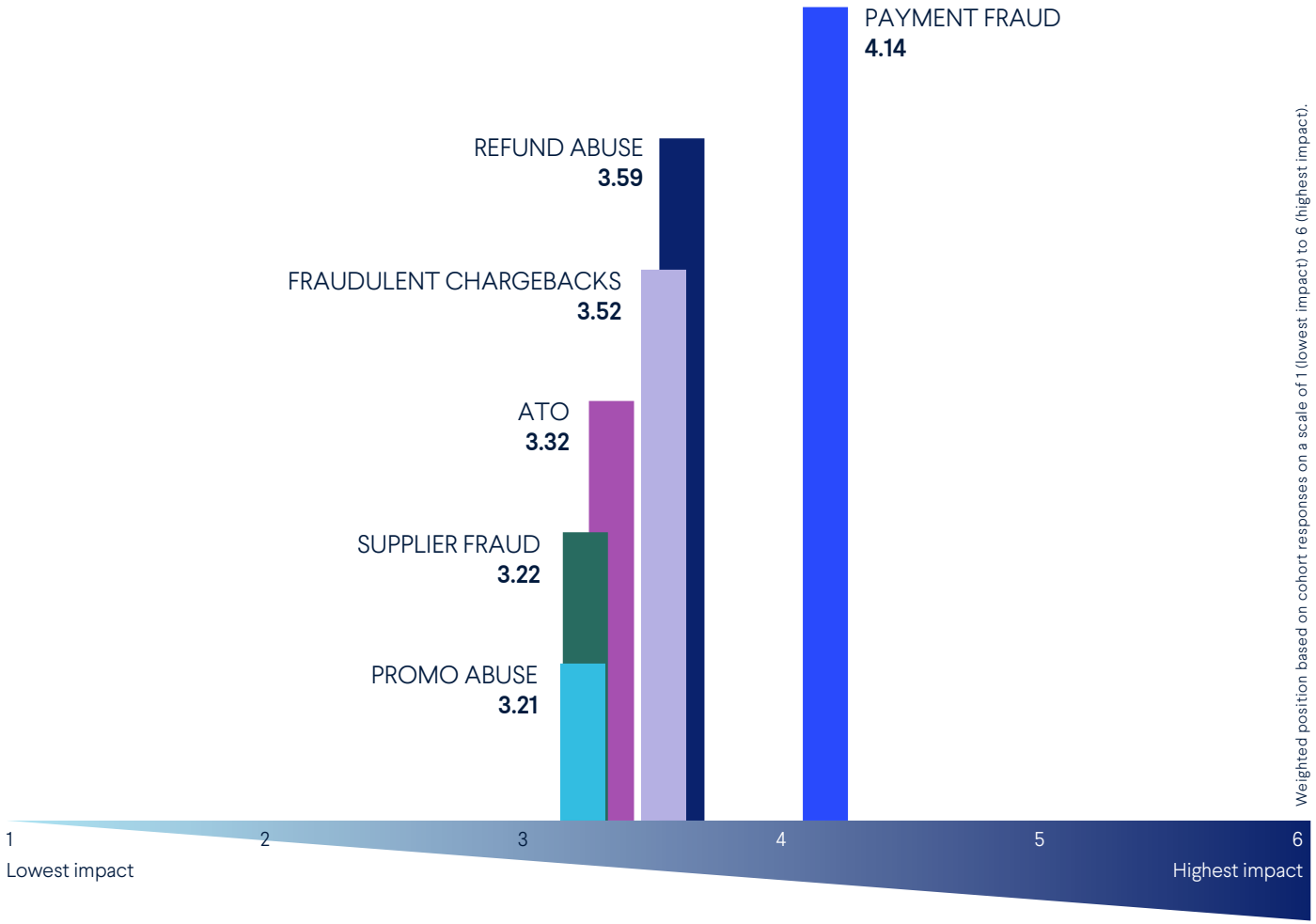


Don't know/NA | Significantly decreased | Somewhat decreased | No change | Somewhat increased | Significantly increased

"How has each of these fraud types changed at your company in the past 12 months? Supplier, partner or seller fraud"

PAYMENT FRAUD & REFUND ABUSE THE WORST TYPES OF FRAUD

TYPES OF FRAUD RANKED ACCORDING TO NEGATIVE IMPACT ON BUSINESS



YEAR-ON-YEAR TRENDS

1. ONLINE PAYMENT FRAUD –
2. REFUND ABUSE ▲
3. FRAUDULENT CHARGEBACKS ▼
4. ATO –
5. SUPPLIER FRAUD ▲
6. PROMO ABUSE ▼

Interesting answers to this question were observed this year, as refund abuse was ranked higher than fraudulent chargebacks as the worst type of first-party fraud, up from the third place in 2025. Perpetrated both by professionals and consumers, **refund and returns abuse is fast becoming a headache** for merchants across verticals.

Meanwhile, supplier fraud ranked slightly higher than promo abuse, up from last year, which could indicate more trouble for Marketplaces.

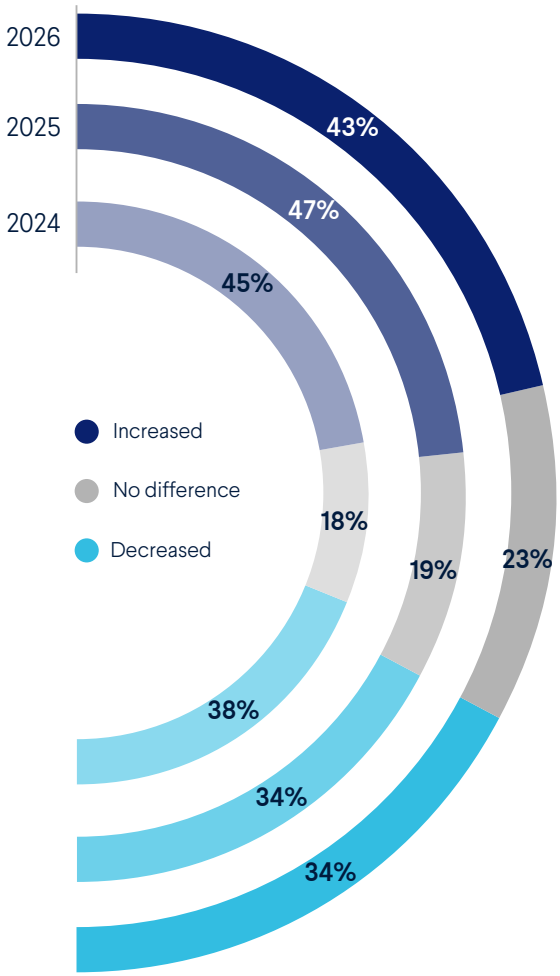
"On average, which of these types of fraud have the worst impact on your business? Arrange the answers in order of impact."

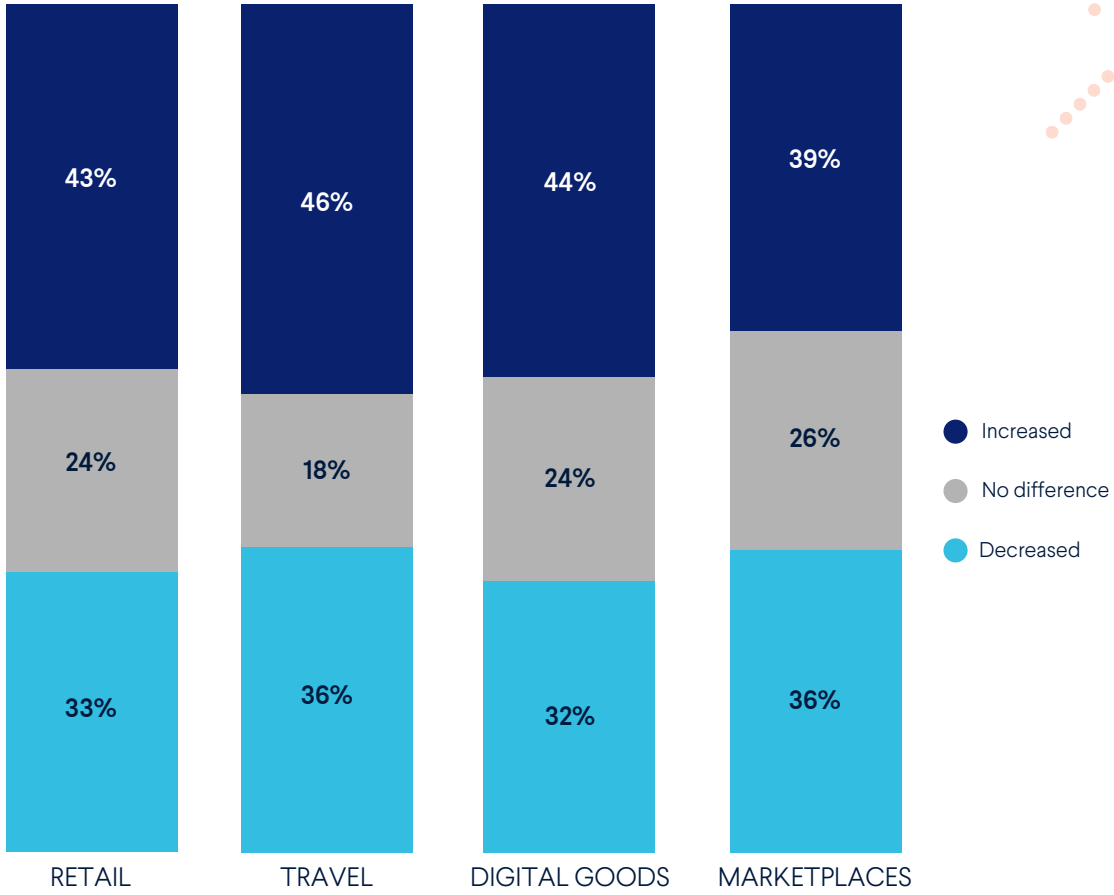
FIRST-PARTY FRAUDSTERS PRESS ON

43%
report a rise in consumer fraud

LIKELIHOOD OF CONSUMERS ATTEMPTING FRAUD

OVERALL





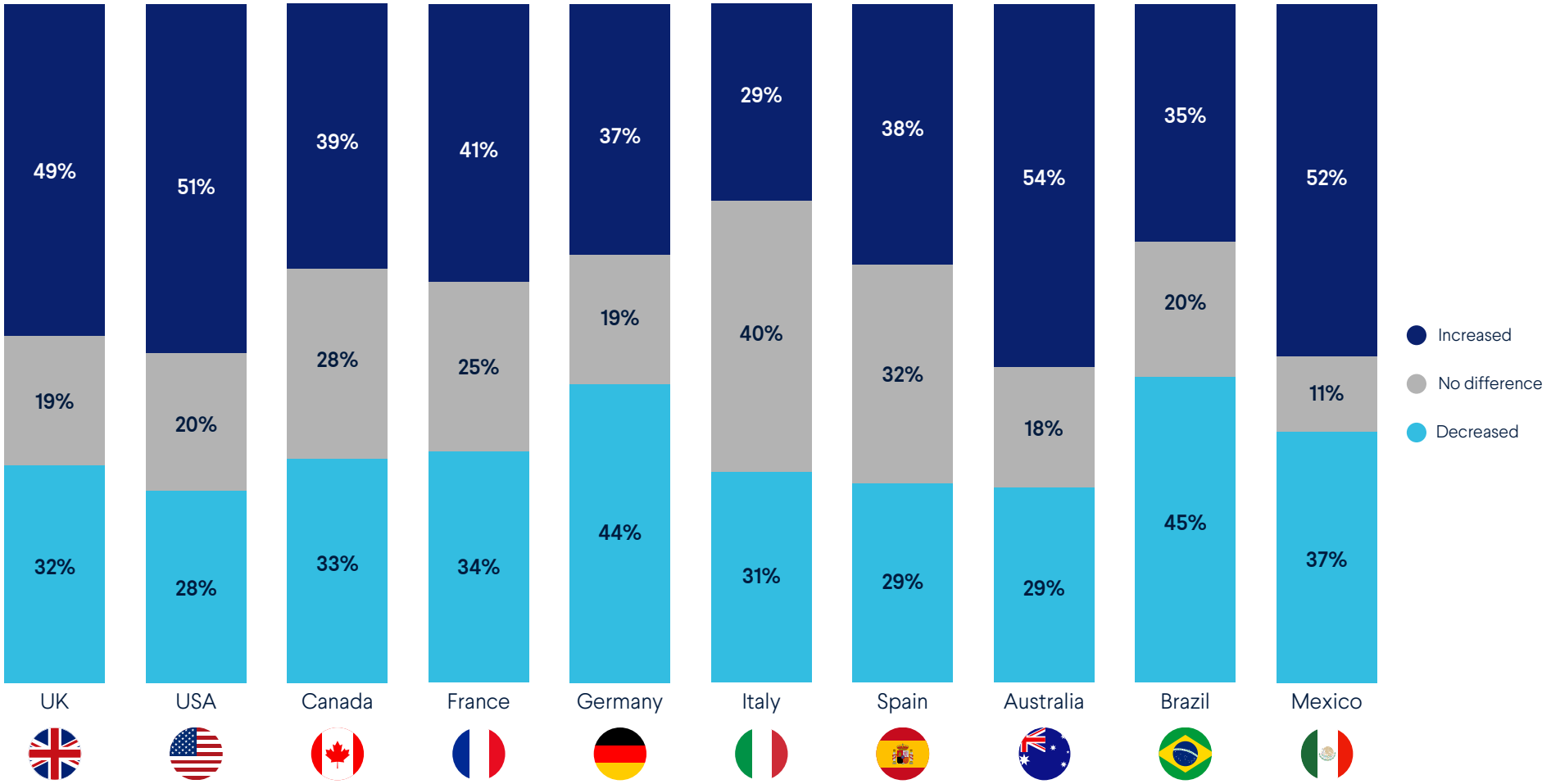
"Have you noticed a change in customer/legitimate cardholder behavior over the past 12 months?"

Merchants continue to see abuse and fraud as a meaningful customer-behavior risk, although the picture appears relatively stable, likely reflecting a balance between increasingly sophisticated tactics, such as AI-generated evidence, and stronger review processes, tighter policies, and more targeted intervention.

Though the overall year-on-year trend in consumer-attempted fraud slightly improved this year, with fewer merchants reporting further increases, country-specific findings vary wildly.

The biggest jumps in fraudulent and abusive consumer behavior were seen in Australia, where 54% of merchants said that consumers are more likely to attempt fraud, followed by Mexico (52%) and the USA (51%). On the other end of the scale, most Brazilian merchants saw a drop in first-party fraud, with 45% reporting reduced likelihood, as did the majority of German survey participants (44%).

LIKELIHOOD OF CONSUMERS ATTEMPTING FRAUD – COUNTRY-SPECIFIC

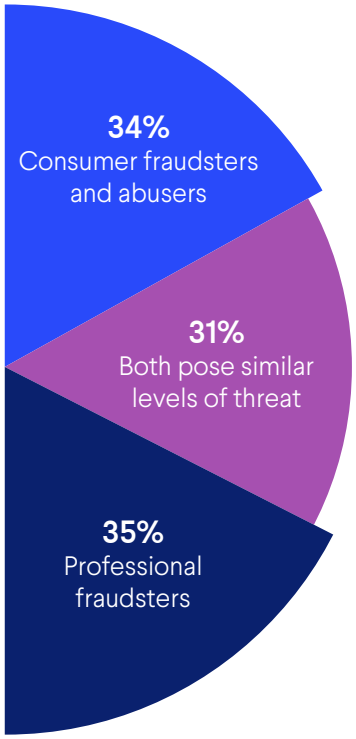


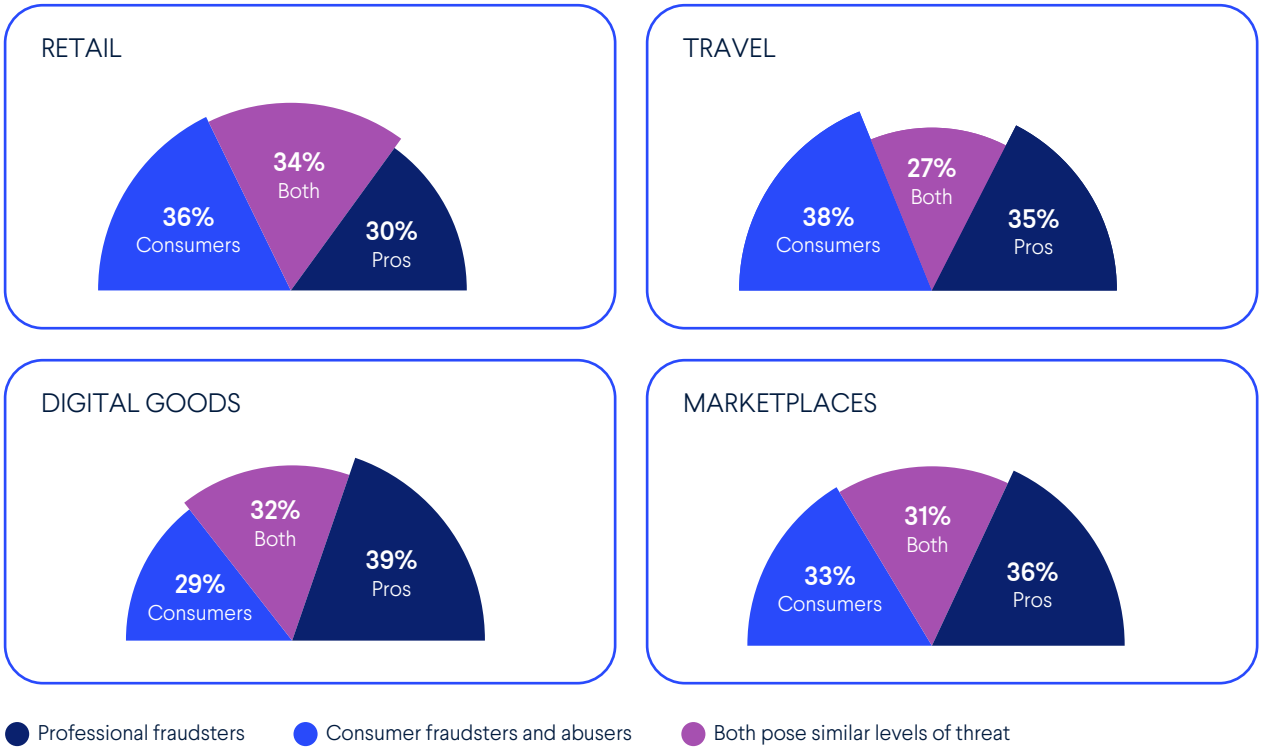
"Have you noticed a change in customer/legitimate cardholder behavior over the past 12 months?"

CONSUMERS AS MUCH OF A THREAT AS FRAUDSTERS, SAY MERCHANTS

BIGGEST PERCEIVED THREAT

OVERALL





"Of the following, who poses more of a threat to your company?"

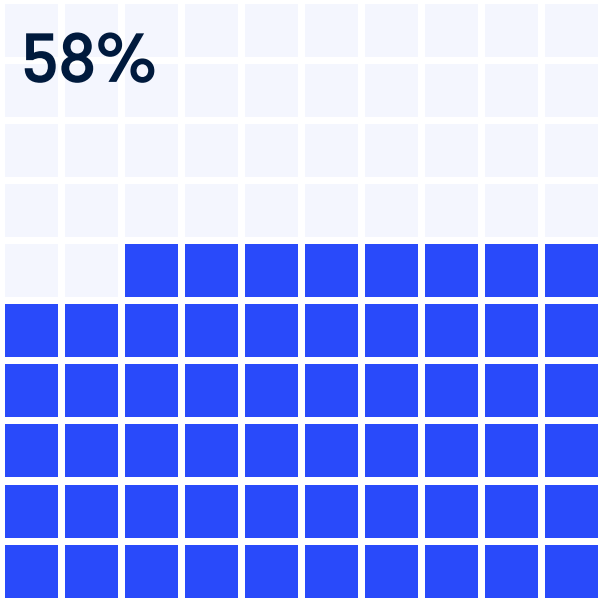
When we asked merchants who posed more of a threat in terms of fraud, opinion seemed evenly split between professional criminals and abusive first parties. This is consistent with a broader fraud landscape in which **traditional fraud threats remain significant, while refund abuse, policy abuse, and other forms of first-party fraud continue to grow in importance**.

Looking at each of our four key sectors in isolation, however, reveals some telling results. Though results are fairly similar, Retail and Travel both scored consumers as of a bigger threat than criminals, giving them the top position. On the contrary, Digital Goods and Marketplaces scored professionals higher.

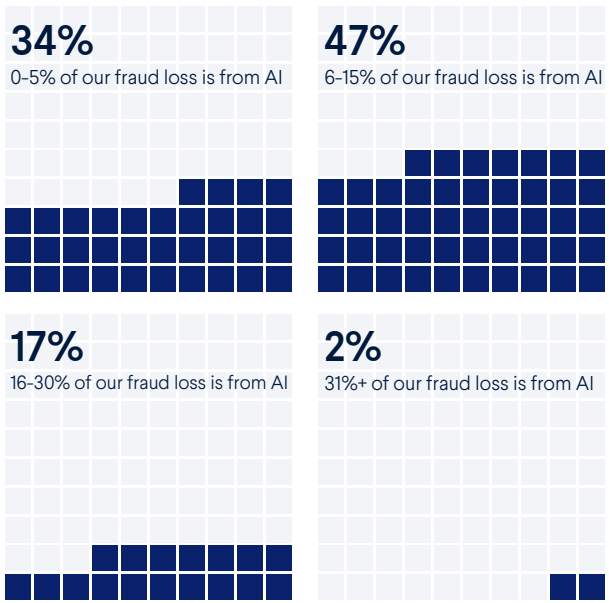
You cannot afford to ignore first-party abuse. Make it integral to your fraud strategy, especially if you're a retailer or travel company.

AI-ENABLED FRAUD AND ABUSE LOOM LARGE

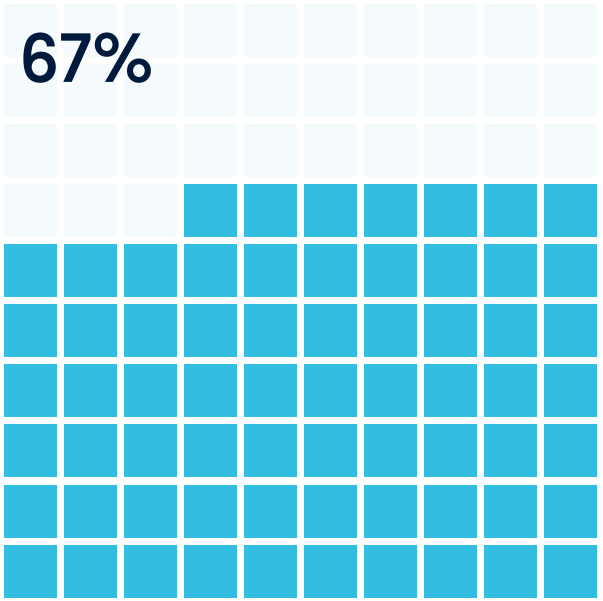
SAW AI USED FOR FRAUD AGAINST THEM IN THE PAST YEAR



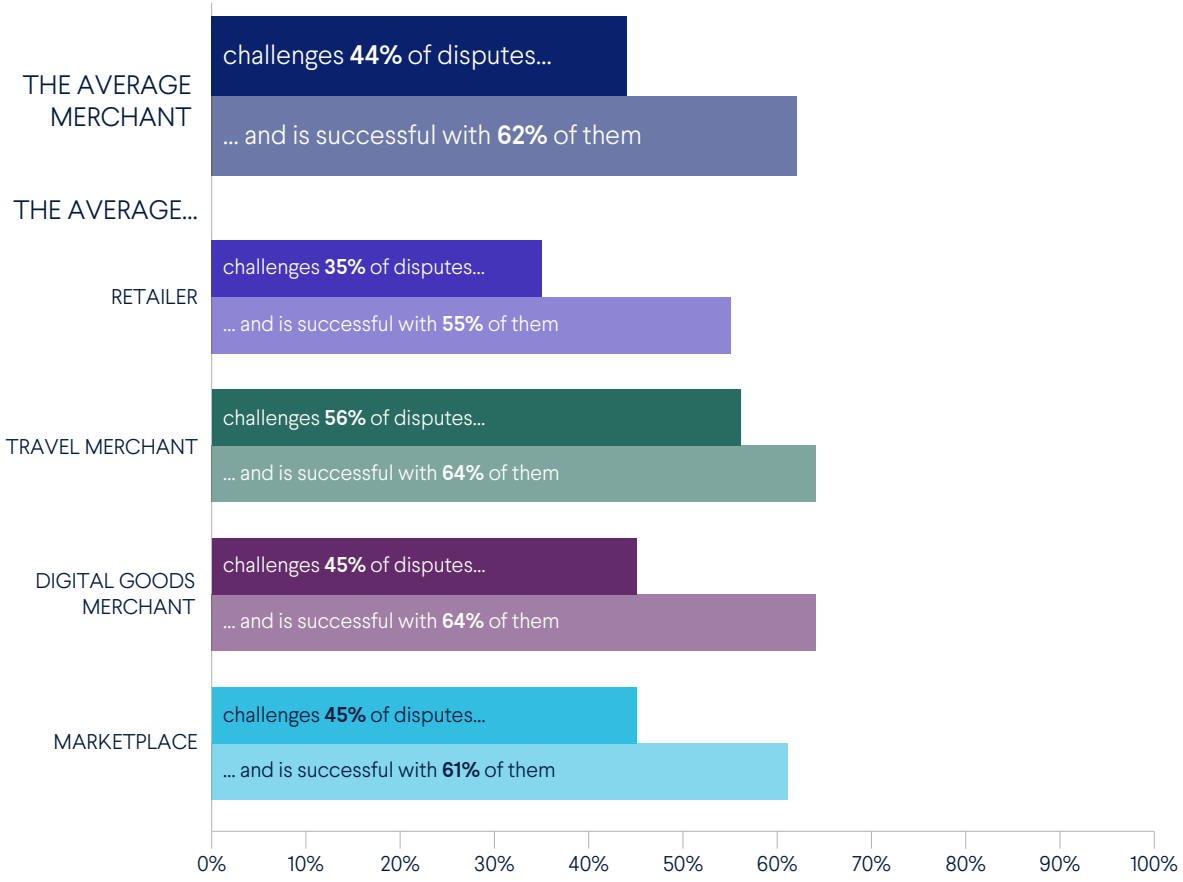
% OF TOTAL FRAUD LOSS ATTRIBUTED TO AI-SUPPORTED FRAUD



RECEIVED AI-GENERATED FAKE REFUND EVIDENCE



ENCOURAGING TRENDS IN CHARGEBACKS AND DISPUTES



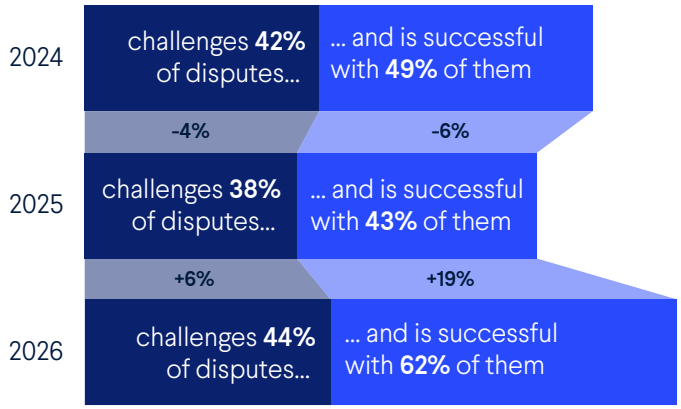
"On average, what percentage of chargeback requests do you challenge?"

"On average, how successful are you with the chargeback requests you challenge?"

Encouraging overall improvements were seen in terms of chargebacks and disputes, **with 6% more merchants challenging disputes and 19% seeing more success** when challenging these disputes compared to 2025.

The rise in both disputes challenged and successful defense rates suggests **merchants are taking a more active and disciplined approach to chargeback management**, likely reflecting stronger evidence, more selective representment, and a greater focus on dispute control under Visa's VAMP framework, even as credit card disputes remain among the hardest to overturn (see next page).

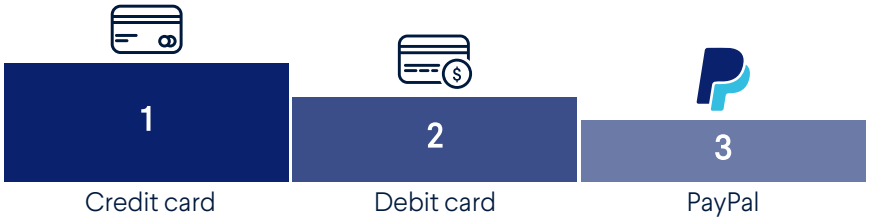
YEAR-ON-YEAR COMPARISON

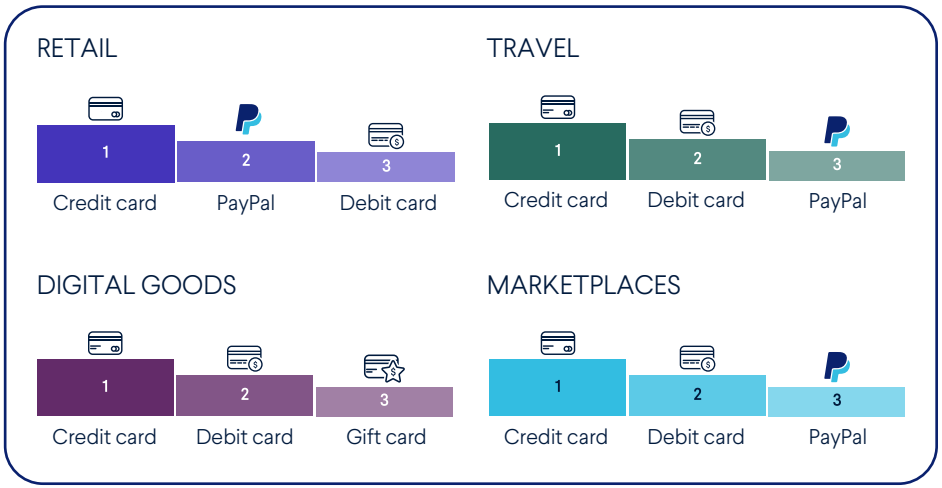


OPPORTUNITIES & BLOCKERS FOR CHARGEBACK CHALLENGES

LEAST SUCCESSFUL PAYMENT METHODS WHEN CHALLENGING DISPUTES

OVERALL



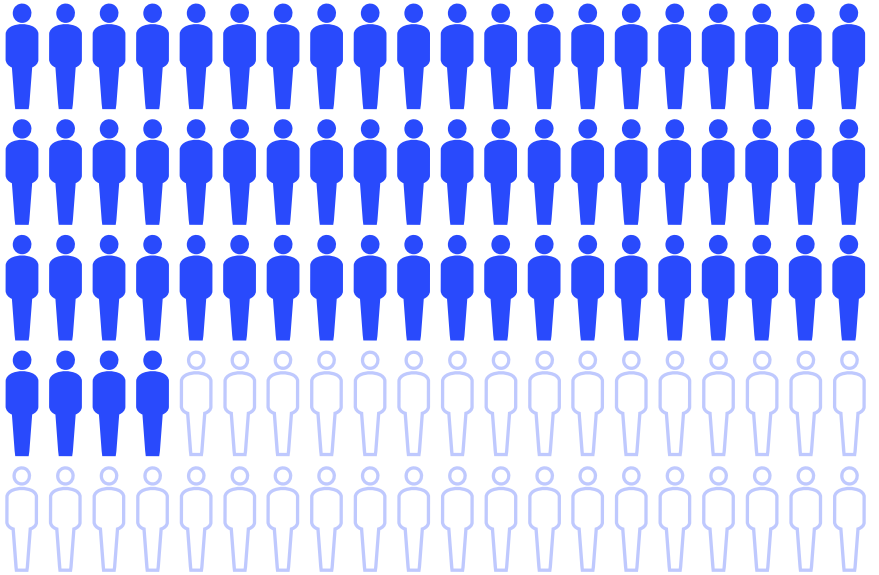


"Which of these payment methods are you least successful with when challenging chargebacks/ disputes? Please select the 2 methods you're least successful with."

> **"As dispute ratios become more commercially important, merchants are likely to weigh the cost of these tools against chargeback fees, operational handling costs, and the wider risk of monitoring exposure."**
>
> Nick Lally, CFO at Ravelin

Our findings on the topic of dispute challenges and pre-dispute alerts clearly show further room for improvement. For instance, could more merchants benefit from pre-dispute alerts? Why are sectors struggling with different payment methods, and what can we learn from each other?

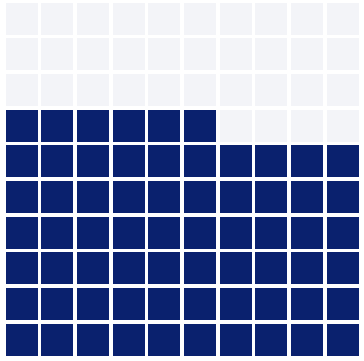
The 64% adoption rate suggests that pre-dispute tools are now a well-established part of chargeback strategy for many merchants.



64% of merchants

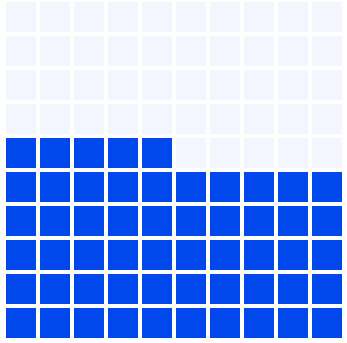
use pre-dispute alerts (e.g. Ethoca, Verifi, RDR).

MERCHANTS REPORT STRUGGLES WITH RETURNS AND REFUNDS



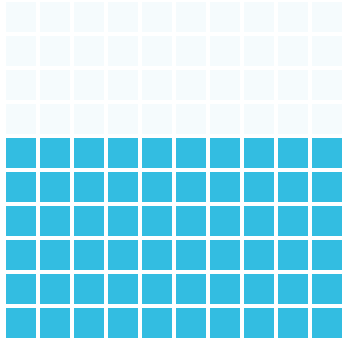
66%

feel pressured to refund customers even when there is evidence they are misrepresenting the quality/condition of items.



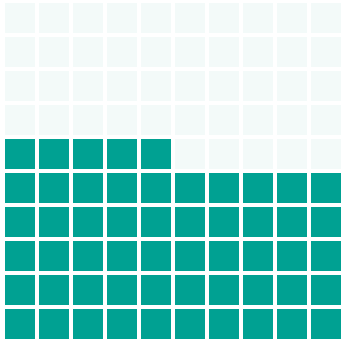
55%

struggle to quantify the scale of their refund abuse/policy abuse problem.



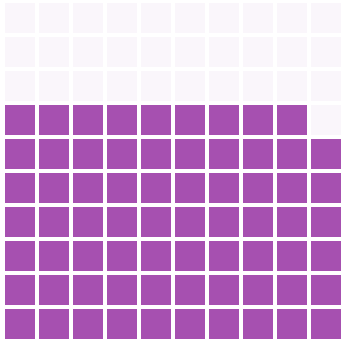
60%

have difficulty telling when a legitimate cardholder is misrepresenting the truth to gain money or items, or making a genuine claim.



55%

say their Customer Service team(s) lack the tools and training to effectively challenge suspicious refund claims.



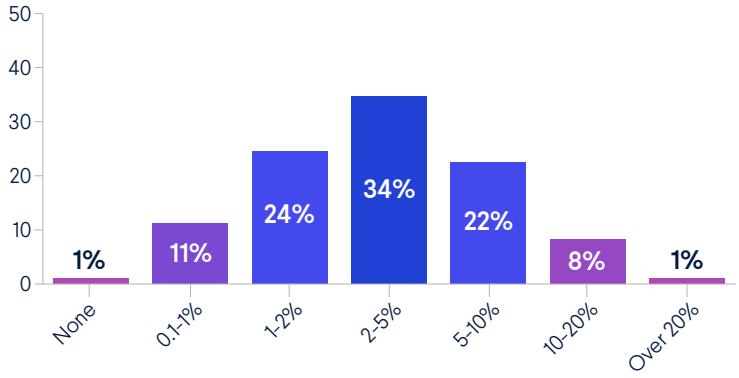
69%

of companies consider customer loyalty and brand reputation more important than stopping refund abuse.

REFUND ABUSE CONTINUES TO PLAGUE ECOMMERCE

Interesting results in this area in 2026. **The majority received requests to refund 2%–5% of their sales**, same as last year. Optimistically, however, overall there was a drop, as many more report refunds between 0.1% and 2% only this year. In a similar vein, merchants now believe fewer of their refunds are abusive – with a notable 11% year-on-year increase in those who estimate this to be less than 1%.

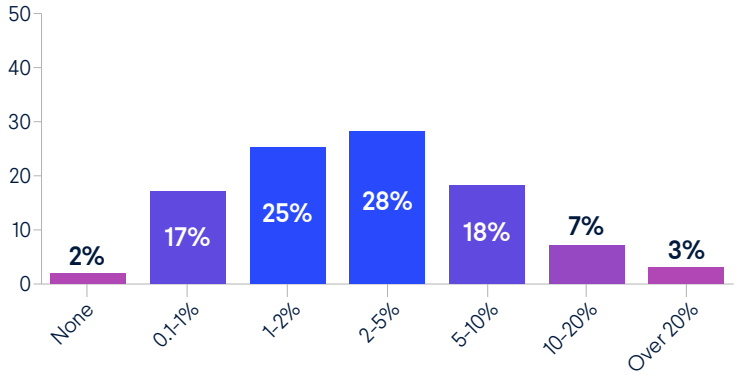
% OF SALES THAT LED TO REFUND REQUESTS



	None	0.1-1%	1-2%	2-5%	5-10%	10-20%	Over 20%
RETAIL	1%	12%	24%	33%	21%	8%	2%
TRAVEL	0%	7%	26%	32%	23%	11%	1%
DIGITAL GOODS	1%	8%	22%	38%	24%	7%	1%
MARKETPLACES	1%	17%	23%	32%	18%	7%	2%

"What percentage of your sales resulted in a refund request over the last 12 months?"

% OF REFUND REQUESTS THAT WERE FRAUDULENT



	None	0.1-1%	1-2%	2-5%	5-10%	10-20%	Over 20%
RETAIL	2%	20%	28%	24%	17%	6%	3%
TRAVEL	2%	11%	25%	30%	19%	10%	2%
DIGITAL GOODS	2%	15%	24%	29%	19%	7%	4%
MARKETPLACES	3%	20%	24%	27%	17%	7%	3%

"What percentage of your returns or refunds in the last 12 months do you estimate are due to policy abuse?"

SECTION C

FIGHTING FRAUD

The report's third section homes in on the tools, strategies and techniques used to fight online fraud.

Discover how confident merchants are in their tech stack and strategy, which tools they use the most, where they stand on the question of friction, and what stops us from doing it all better.

You'll develop a better understanding of how ecommerce detects fraud in 2026 – and how to improve your performance.

KEY FINDINGS

30%
still don't use any AI against fraud

66%
wish to do more to stop fraud

friction & public image
the main blockers of fraud prevention

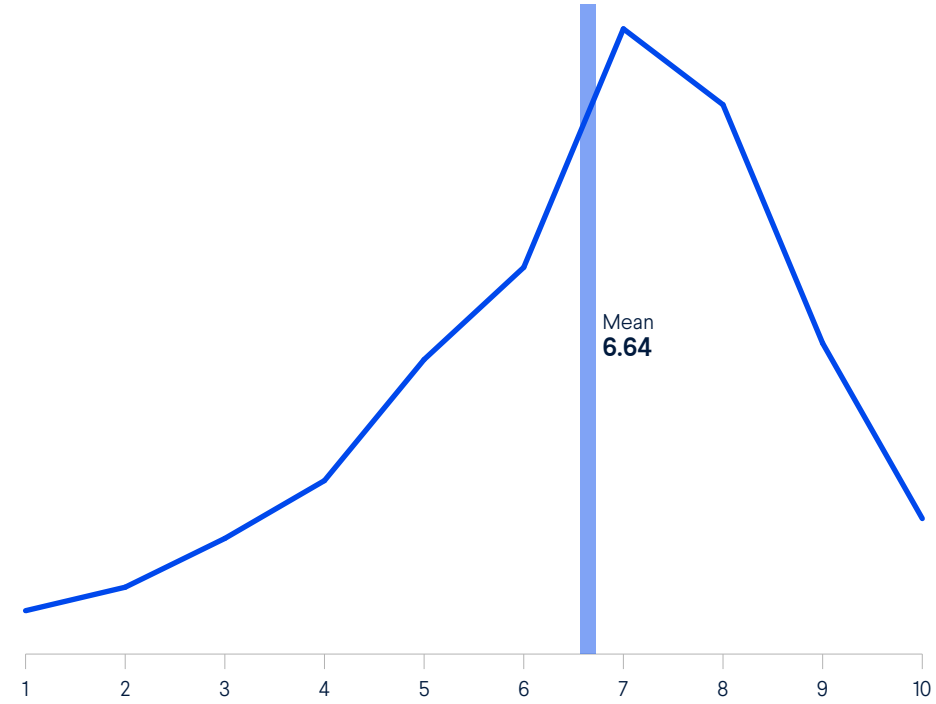
MODERATE-HIGH CONFIDENCE IN FRAUD TECH STACK AND STRATEGY REPORTED

Do merchants find their tech and techniques to be a good match for fraudsters? As a new question for 2026, we asked merchants to rate their confidence levels in their fraud detection tech stack from 1 to 10, as well as their confidence in their fraud strategy.

Although the results were fairly positive, they average at around 7 out of 10 for both questions, with fraud strategy confidence slightly higher than tech stack confidence. That the two findings largely mirror each other is also interesting, as it demonstrates that the issue does not lie solely with technology or solely with strategy either.

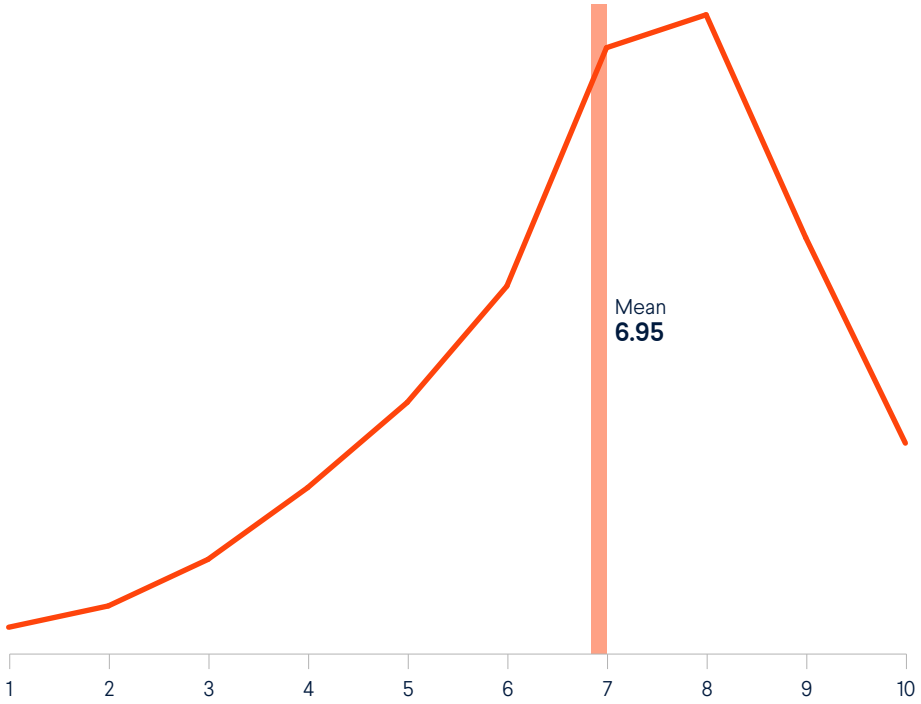
The message is clear: **Most merchants do not feel the degree of confidence that they should from their fraud detection setup**. Your fraud detection vendor ought to be a partner, enabling your strategy and supportive proactive defenses.

CONFIDENCE IN FRAUD TECH STACK



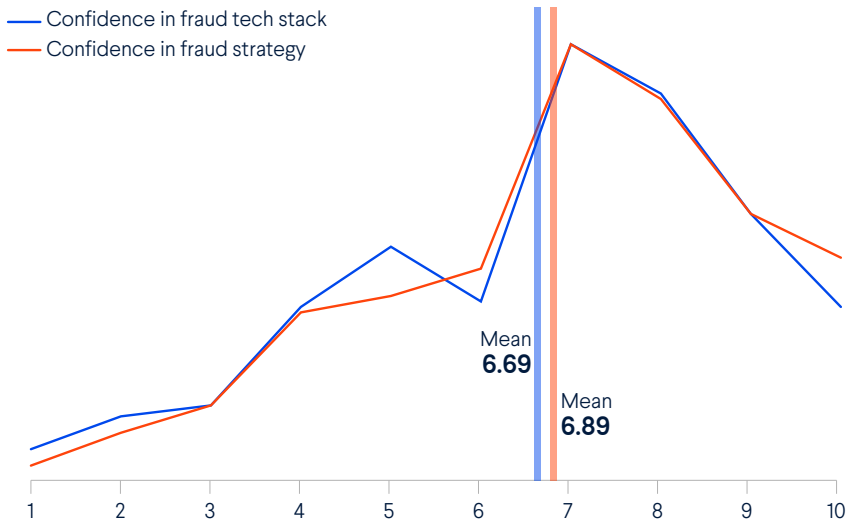
"On a scale of 1 to 10, how confident are you in your fraud tech stack?"

CONFIDENCE IN FRAUD STRATEGY

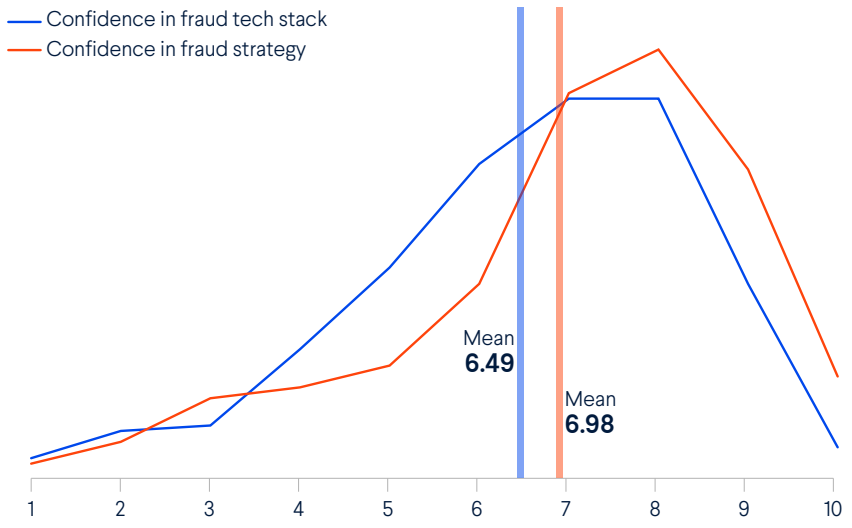


"On a scale of 1 to 10, how confident are you in your fraud strategy?"

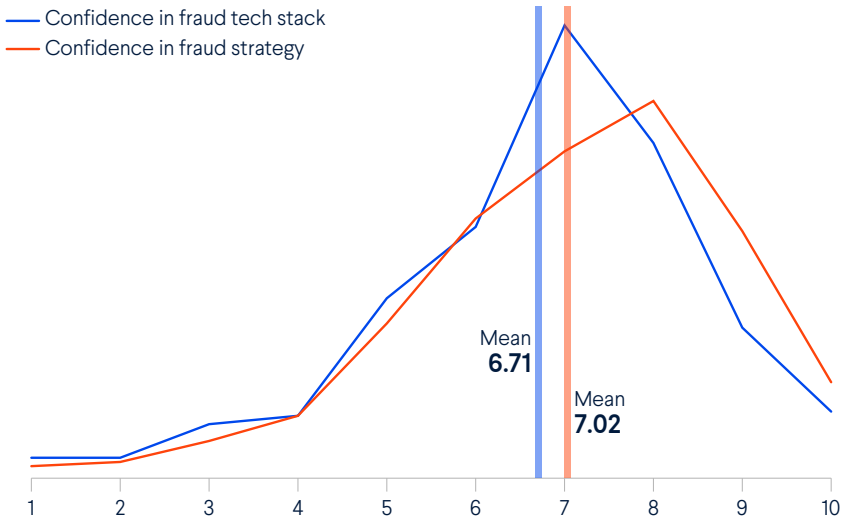
RETAIL



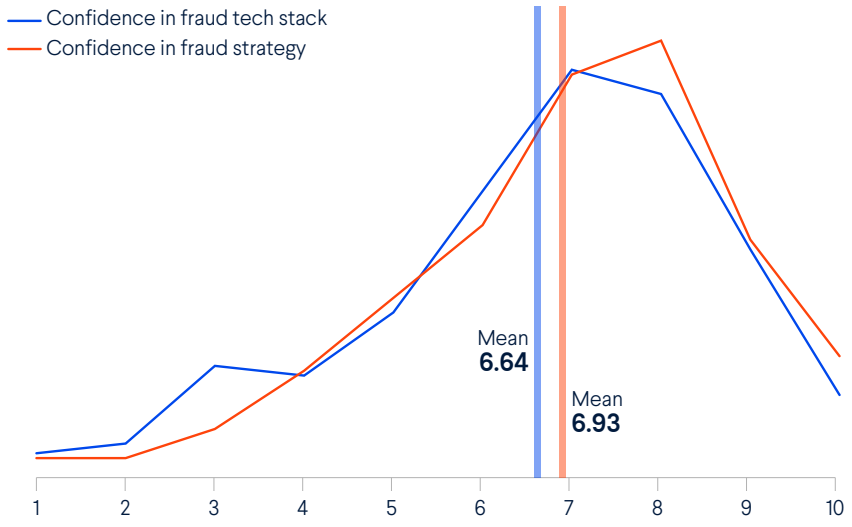
TRAVEL



DIGITAL GOODS



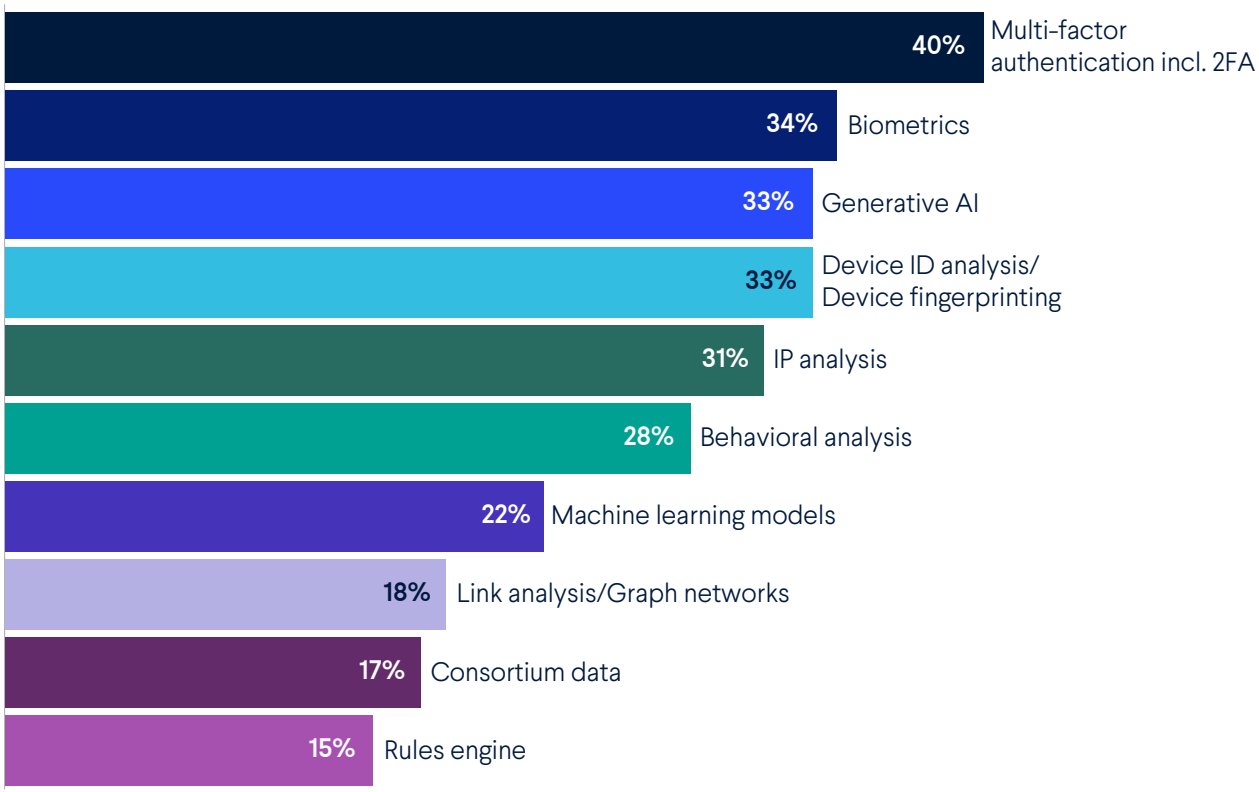
MARKETPLACES



"On a scale of 1 to 10, how confident are you in your fraud tech stack/fraud strategy?"

ANTI-FRAUD TOOL PREFERENCES VARY – IS ML OVERLOOKED?

MOST EFFECTIVE TOOLS AS CHOSEN BY MERCHANTS



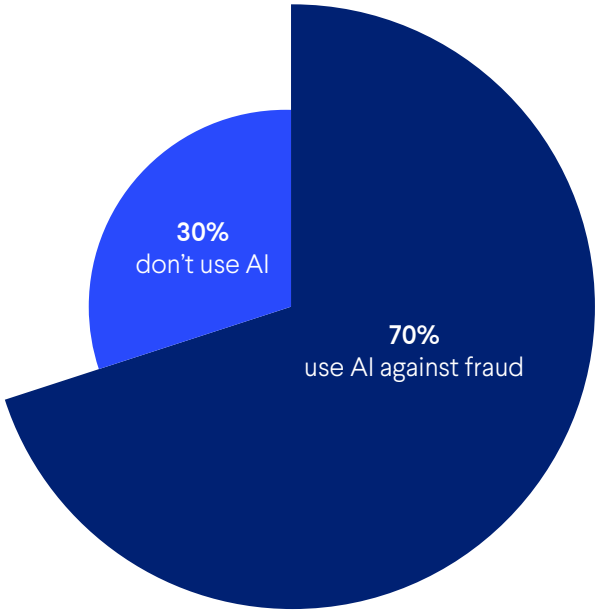
"Which of the following tools do you find most effective for fighting fraud? Select up to 3 tools."

Multi-factor authentication, including 3D Secure technology, was voted the top fraud fighting technology for one more year, followed by new entry Biometrics.

In third place is GenAI tech with 33% of the vote, yet also AI-based machine learning (ML) only scored 22% and was a much less popular choice. Graph network link analysis, a key technology for fraud detection, has also not featured very high.

Combined with our finding that 3 in 10 enterprises don't use machine learning

% OF MERCHANTS USING ANTI-FRAUD AI



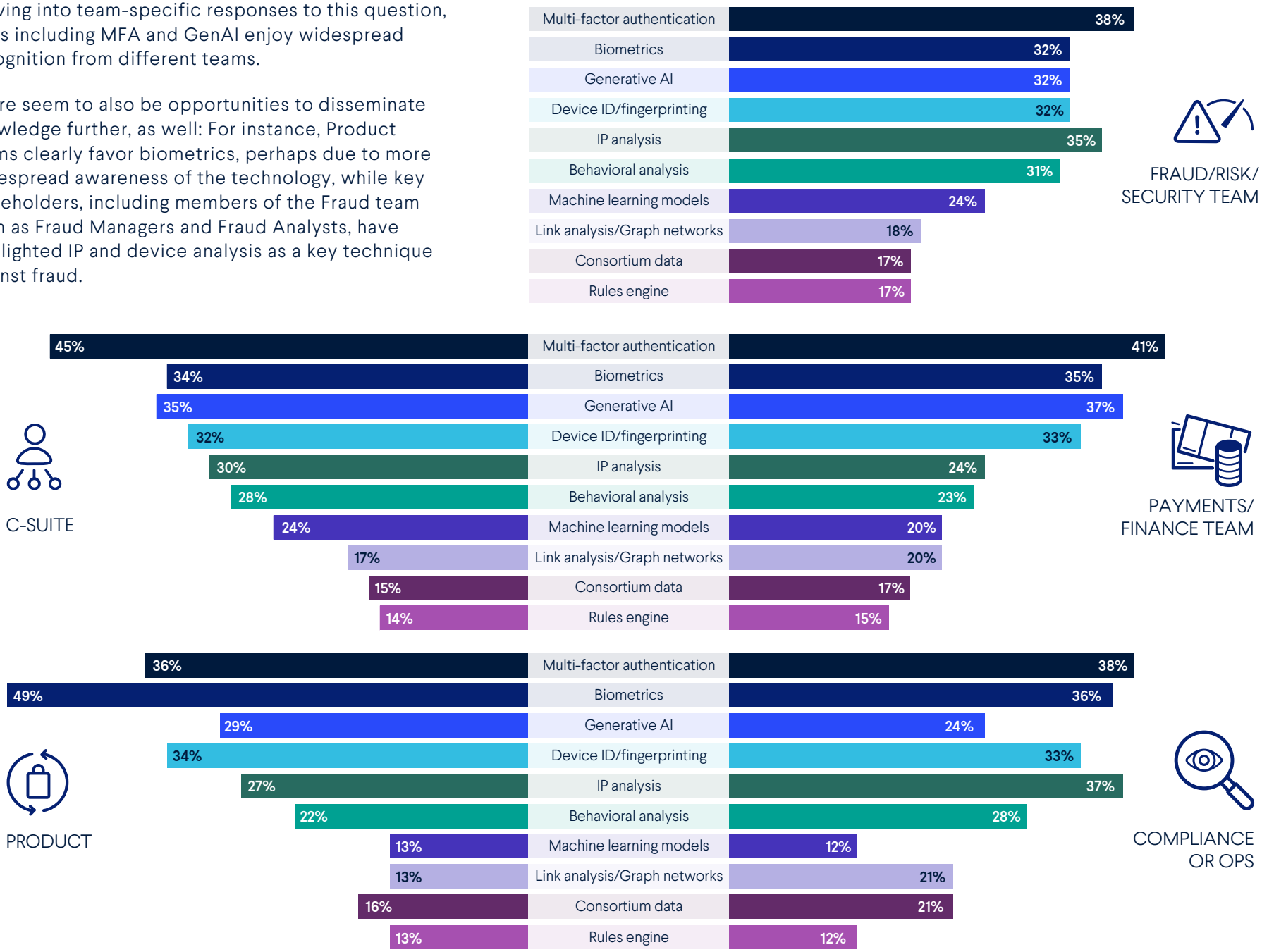
"Are you currently using machine learning (ML), large language models (LLMs) or any other AI tech to detect/prevent fraud?"

automation to scale their anti-fraud operations, **are merchants making the most of available cutting-edge tech?**

It's up to the entire community to exchange knowledge and information.

Delving into team-specific responses to this question, tools including MFA and GenAI enjoy widespread recognition from different teams.

There seem to also be opportunities to disseminate knowledge further, as well: For instance, Product teams clearly favor biometrics, perhaps due to more widespread awareness of the technology, while key stakeholders, including members of the Fraud team such as Fraud Managers and Fraud Analysts, have highlighted IP and device analysis as a key technique against fraud.



DYNAMIC FRICTION FAVORED, BLOCKING A CLOSE SECOND

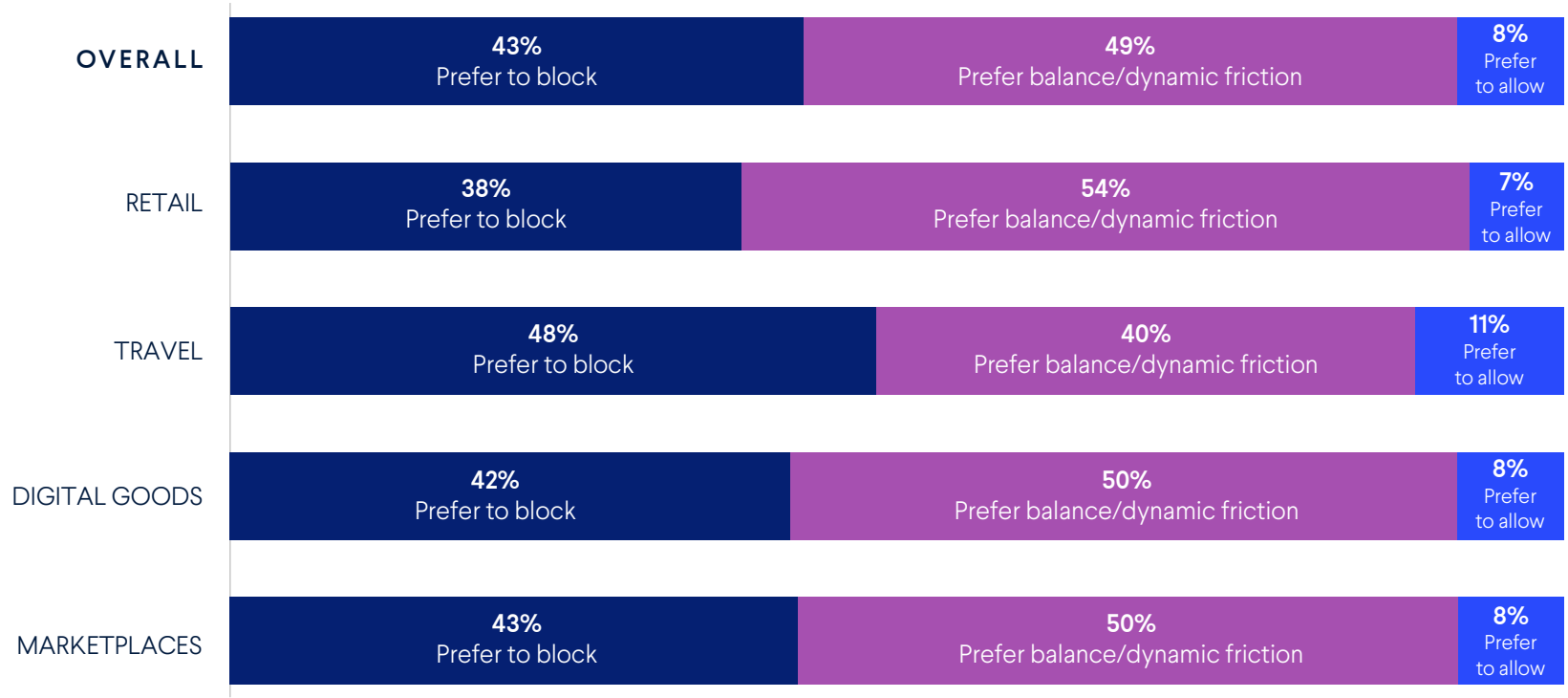
The question of friction, false positives and customer insults in fraud detection and payments is as long as the technology itself – so we also asked merchants for their preferences: **safer transactions or more transactions?**

I prefer to **block** as many fraudsters as possible, even if it means introducing friction into the journey of legitimate customers (potentially affecting customer loyalty and satisfaction)

I prefer a balance of the two/**dynamic friction**

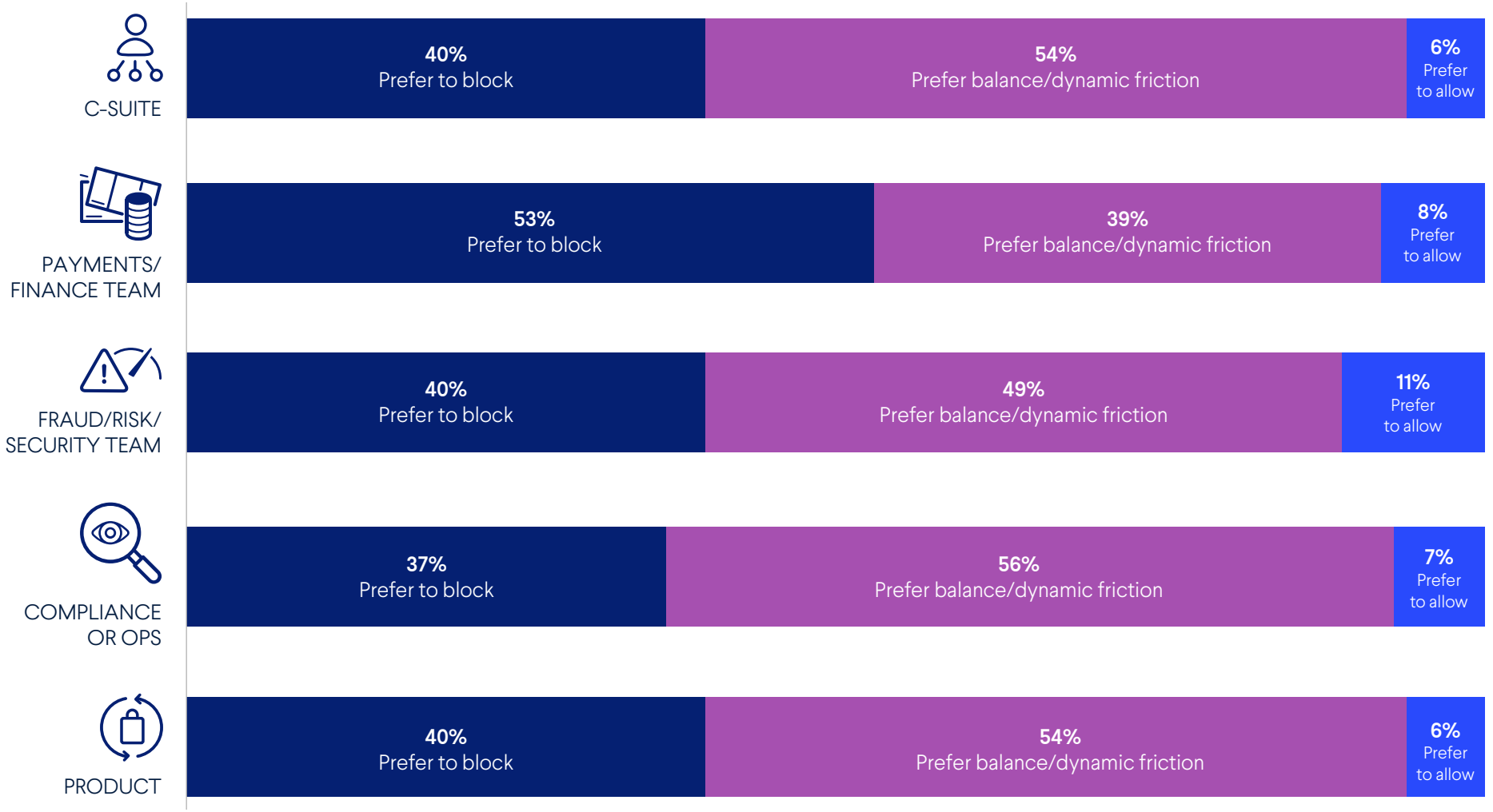
I prefer to **allow** as many customers as possible, even if it means letting some fraudsters get away with it (potentially affecting revenue)

MERCHANT PREFERENCE ON FRICTION VS CONVERSION



"Where do you stand on friction vs security when it comes to online purchases?"

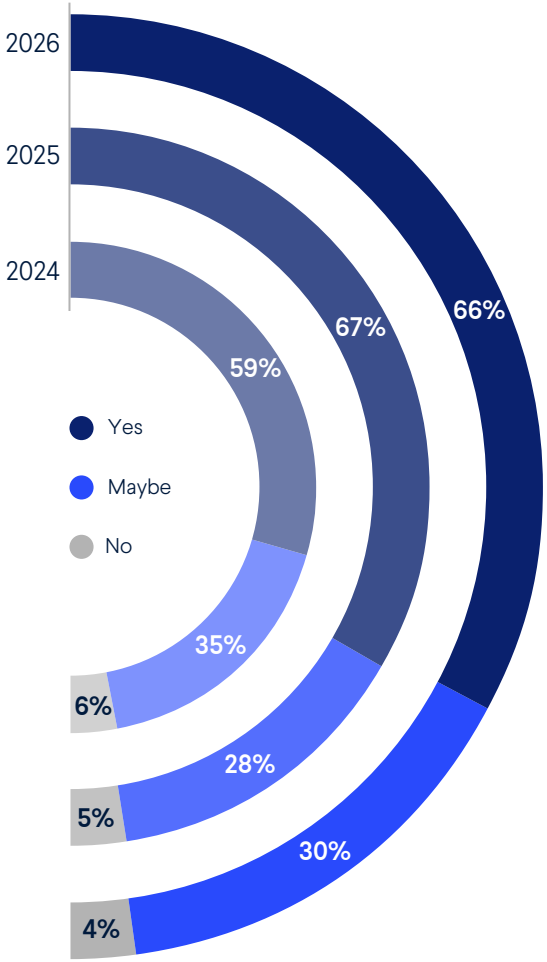
TEAM PREFERENCE ON FRICTION VS CONVERSION



WE COULD DO BETTER, SAY MERCHANTS

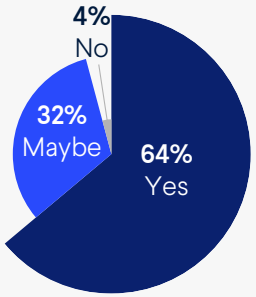
% WHO BELIEVE THEIR COMPANY SHOULD DO MORE AGAINST FRAUD

OVERALL

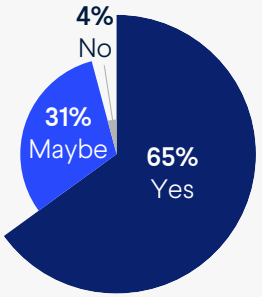


"Do you believe your company should be doing more to battle fraud?"

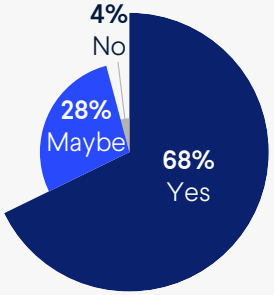
RETAIL



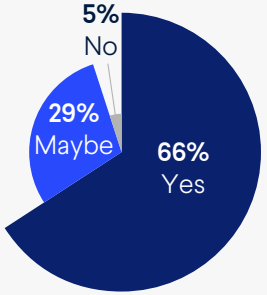
TRAVEL



DIGITAL GOODS



MARKETPLACES



Most merchants believe they should, or probably should, work harder to stop fraud – with less than 5% responding negatively.

Despite some year-on-year improvements noted in responses to other questions, here, 2026 results were very consistent with recent years: **There is more work to be done for the fraud-fighting community, both to deal with current fraud and prepare for the future.**

FRICTION, IMAGE & RESOURCES ARE THE BIGGEST BLOCKERS

PERCEIVED OBSTACLES TO BETTER FRAUD DETECTION



29% Concerns about customer friction
29% Concerns about public image
24% Lack of developer/IT resources
24% Legacy and/or unsuitable technology
24% Operational inefficiency
23% Lack of executive priority
22% Budget constraints
20% Data visibility gaps
20% Talent shortage
13% Siloed internal teams
9% We are as effective in fighting fraud as we can be

only **22%** say budget stops them from fighting fraud better

Several blockers have been identified by respondents, with less than 1 in 10 claiming they are as effective as can be.

Customers seem to be at the heart of these, as the top choices involved a fear of blocking good orders and reducing conversions, as well as a perception that public image could be harmed by more aggressively blocking fraud.

However, this year as well as in previous issues, we have seen this report highlight how public image can be severely harmed when a company falls victim to fraud. Admittedly, some fraud strategies and solutions are better at powering growth than others – **they don't have to be a blocker**, though.

This ties in with another prominent type of obstacle: unsuitable technology and lack of developer resource. A good fraud vendor will work with you, not against your resources, to enable an integration that can achieve the best results from as much data as possible.

"In your opinion, what stops your company from being more effective in fighting fraud? Please select up to 3 answers."

SECTION D

THE FUTURE OF FRAUD

In the final section of this report's findings, our eyes are firmly set on the future.

How do our merchants believe the fraudscape will evolve and shift in the next year and further? Which types of fraud do they predict will rise, how will agentic commerce affect ecommerce, and what are the biggest challenges coming up?

Read this to discover the questions you should be asking to future-proof your operations.

KEY FINDINGS

Over half
expect fraud to rise in 2026

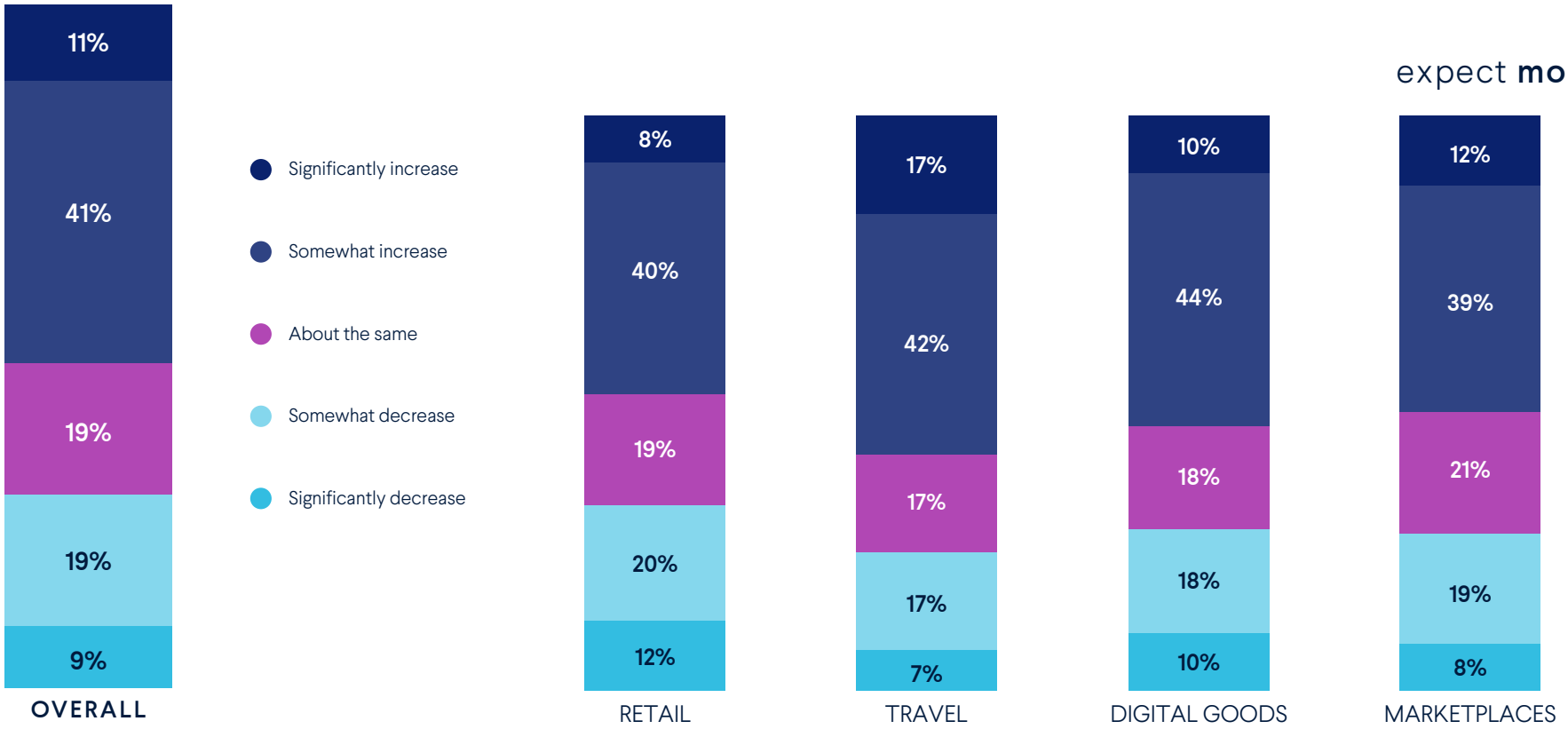
8 in 10
believe the cost of fraud will increase

AI
selected as the main fraud challenge coming up

FRAUD PREDICTED TO RISE – BUT THERE'S OPTIMISM, TOO

FUTURE FRAUD EXPECTATIONS

52%
expect **more** fraud



"Do you expect fraud against your company to increase or decrease in the next 12 months?"

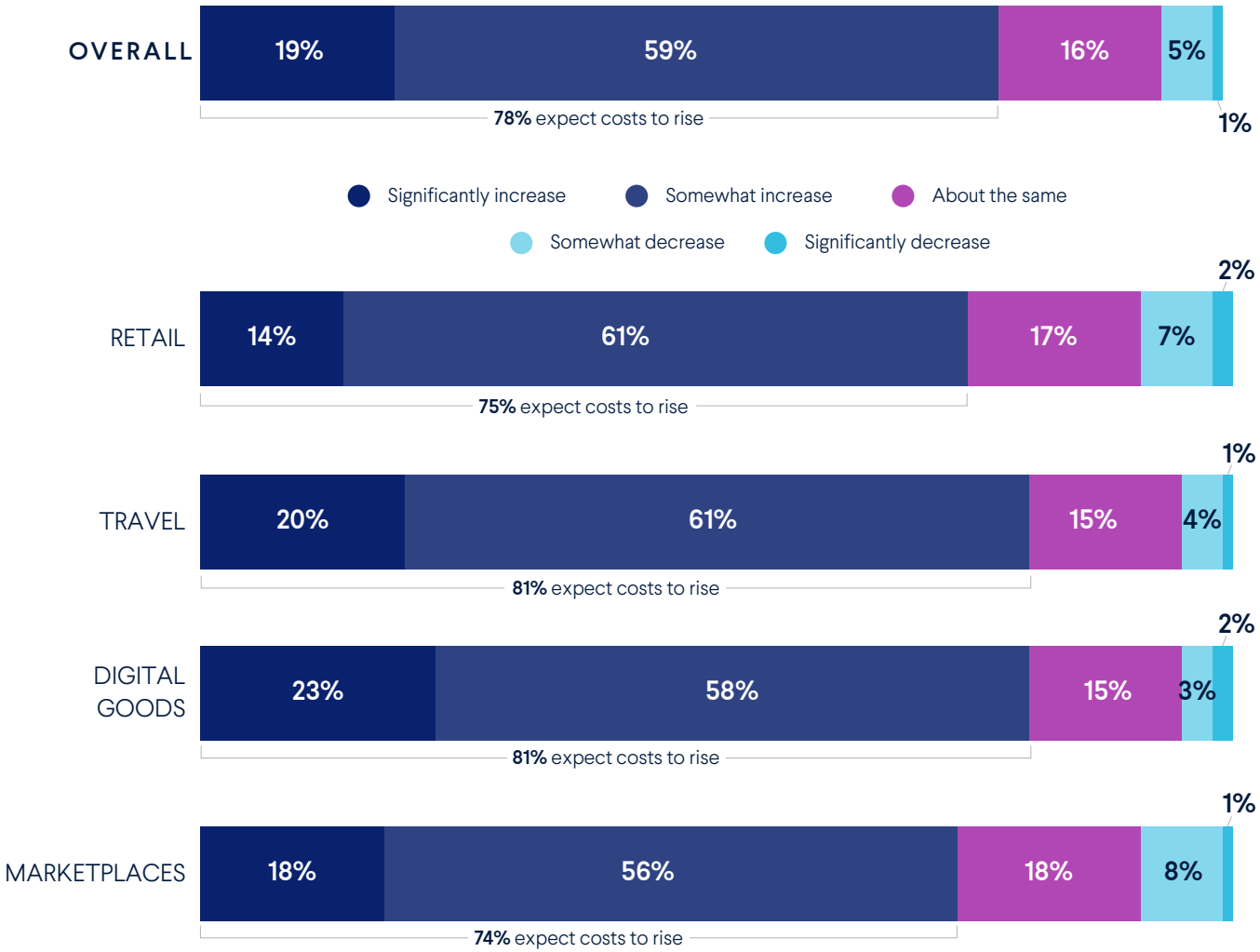
Evidently, there is an air of optimism in future predictions in 2026 where, although a majority of 52% expect fraud to increase this year, this is significantly lower than last year's expectations.

While 52% of merchants still expect fraud pressure to rise overall, a greater share now expect stability or decline compared to last year's predictions. Almost 3 in 10 expect to see less fraud in the next 12 months.

This may reflect growing confidence in stronger controls, increased automation, and more mature data-led fraud management, even as fraud remains a persistent business risk. Retail was the most optimistic and Travel the most pessimistic sector.

8 IN 10 EXPECT FRAUD COSTS TO RISE

Y-O-Y FRAUD LOSS PREDICTIONS



"In the next 12 months, do you expect to spend more or less on combating fraud, including tools/solutions, contractors, fraud loss, resources, etc.?"

78%
predict increased cost of fraud

Across the board, with 78% of respondents in agreement and only 1–2% expecting to spend significantly less, the consensus is clear: **The cost of fraud is rising.**

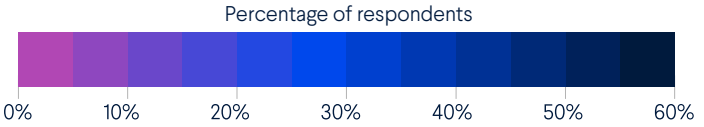
Notably, Digital Goods and Travel are the most impacted sectors, both sitting at a 81% increase prediction. Marketplace and Retail show slightly more tempered though still overwhelmingly negative outlooks for the financial impact of fraud.

PAYMENT & FRIENDLY FRAUD TO RISE?

Reasonably, **most respondents expect fraud to rise**, though it's interesting to note that certain types seem to have plateaued. Payment fraud remains the dominant concern, yet merchants observe that **consumer fraud has shifted its focus, and is getting worse**: Fraudulent first-party chargebacks are now in the third place, expected to increase less than refund abuse, which has entered the top 2. The high "No change" sentiment for ATO and partner/seller fraud suggests they are viewed as persistent threats rather than emerging spikes.

PREDICTIONS BY FRAUD TYPE

Average sentiment score*		Significantly increase	Somewhat increase	No change	Somewhat decrease	Significantly decrease
+0.63	Online payment fraud	22%	42%	16%	14%	5%
+0.41	Chargeback fraud	15%	37%	25%	14%	8%
+0.38	Account takeover attacks (ATO)	14%	31%	31%	16%	9%
+0.23	Promo, voucher & policy abuse	13%	32%	30%	18%	8%
+0.23	Refund abuse	17%	36%	24%	14%	9%
+0.09	Supplier, partner & seller fraud	10%	29%	34%	18%	10%



* A positive score indicates a net expectation of growth in that fraud type. Weighted score calculated between +2 (Significantly increase) to -2 (Significantly decrease), with 0 denoting "No change".

"Which types of fraud do you think will increase in the next 12 months, and by how much?"

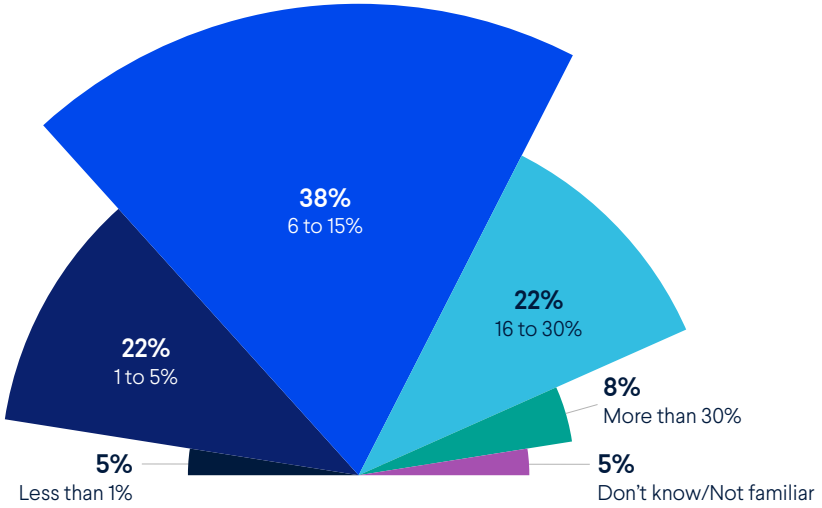
AI INSPIRES MORE TRUST THAN HUMANS

WHO IS MORE TRUSTWORTHY AS A SHOPPER?



"As a merchant, who do you think is more trustworthy? Do you consider AI shopping agents more or less trustworthy than traditional transactions initiated by human customers?"

AGENTIC SHARE OF ECOMMERCE TRANSACTIONS BY 2029



"What percentage of your total ecommerce transactions volume do you predict will be initiated by autonomous AI agents within the next 3 years (by early 2029)?"

Most readers will be well aware of the prevalence of agentic AI shopping in industry conversations. Tech giants are building protocols to support ways for AI to buy their items and services on behalf of consumers – with a seemingly endless parade of enticing proposals to allow this to happen safely, confidently and with clarity of responsibility. Yet, **at the moment, nothing is decided**.

The majority of merchants find AI more trustworthy than human consumers. And although this is testament to the level of confidence in agentic protocols, it can be assumed that the perceived **breakdown of trust between merchants and consumers has also contributed to this result**, thanks to the ever-rising rates of chargeback fraud, refund abuse and other first-party schemes.

Merchants are evidently beginning to view autonomous AI agents not as a fringe concept, but as a credible and potentially trusted future transaction channel.

We have plenty more findings and analysis to share with you around agentic AI commerce, trust, and fraud. To get all the data, follow this link to **Ravelin's Agentic Commerce & Fraud** report, released in April 2026.

AI CROWNED THE BIGGEST FRAUD CHALLENGE COMING UP

We also asked merchants to tell us the **biggest fraud challenge** that's coming up for their company, in their own words.

1 in 3

responses to this question brought up

artificial intelligence

Here are some examples:

"The fact that fraud is already being committed using AI complicates things considerably."

"The use of AI to modernize fraud, taking advantage of the current knowledge gap."

"AI is smart and AI is making fraudsters more creative."

Other interesting responses include:

"It's getting harder to spot the real threats in all the noise."

"Faster fraud resolution cycles that surpass traditional monitoring and manual checks."

"Balancing tighter fraud controls with customer trust and experience is getting harder"



Word cloud featuring the most common words in the responses to the question *"What do you consider to be the biggest fraud-related challenge coming up for your company?"*

SECTION E

FINDINGS & FRAUDSCAPE ANALYSIS BY RAVELIN'S CO-FOUNDERS



FINDINGS & FRAUDSCAPE ANALYSIS BY RAVELIN'S CO-FOUNDERS

Martin Sweeney, Mairtin O'Riada and Nick Lally comment on the findings of this year's fraud survey, the 2026 fraudscape, and what's next.



Martin Sweeney
CEO at Ravelin



Mairtin O'Riada
COO at Ravelin



Nick Lally
CFO at Ravelin

AN UNEVENLY DISTRIBUTED REVOLUTION

We're living through a time of great change, but this technological revolution is unevenly distributed.

Certainly, consumers are loosely aware of AI. Maybe they've used ChatGPT a few times to write a poem or draw a picture. They then think "that's a nice toy", go back to their lives and forget about it.

Many consumers find it hard to conceive what all the fuss is about, and predictions of world-changing technology bemusing or typical technology industry hype. That's one end of the spectrum of AI adoption.

AI maximalists, by contrast, are using AI to deliver every part of their jobs – to a greater or lesser degree of success. There is considerable space between these disparate camps.

And there are industries for which AI already is truly revolutionary. Trying to predict which industry will be disrupted and precisely how is a futile game, though we can make educated guesses.

Early signs show that software engineering may have one of the biggest changes out of almost every industry, and this includes fraud detection.

In fact, anything that involves repetitive work is a fantastic candidate for agentic automation – not knowledge work as much as *procedural* work.

But the question is, what comes

> **Fraud perpetration is in that category of disciplines that are perfect candidates for agentic AI automation.**

next? Which other industries, which other technologies are a natural fit for the capabilities of AI systems?

PROCEDURAL RISK & ASYMMETRIC AI ADOPTION

Fraud perpetration is largely a procedural task. A highly skilled fraudster will have some proprietary domain knowledge and may be frequently experimenting with new techniques, but these techniques still need to be deployed at scale – procedurally – to be successful.

In other words, they need to commit fraud really well, over and over again, to evade detection, to come up with the cleanest-looking data, to make their efforts financially sustainable, and to get around automated detection systems.

That is a procedural exercise for organized crime. It is highly automated. Fraud perpetration is in that category of disciplines that are perfect candidates for agentic AI automation.

> **It is highly likely that the metrics used by merchants to catalog fraud are no longer fit for purpose.**

With one in three merchants not using AI or machine learning as part of their defenses, it is very probable that career fraudsters are adopting AI faster than all but the most nimble businesses.

The reasons are primarily operational and systemic: Fraud and revenue protection teams often have to compete with other departments for resources, and internal compliance also takes time.

On the other hand, criminals are markedly more agile. Unlike an ecommerce enterprise, which may have competing interests and a complex operating model, an online fraudster has a very constrained problem space for AI and a very clear definition of success. The cost of failure for a criminal is lower as well.

And this asymmetric adoption by fraudsters and enterprises can – and will – lead to more successful attacks. In fact, we may already be seeing this but finding it hard to enumerate.

From the perspective of the merchant, it is difficult to know precisely which fraud is AI-powered or supported and which is not. Our survey, however, found that 58% of merchants believe it is already happening. In fact, 67% said they have received fake refund evidence, in particular.

THE PARADOX OF FRAUD LEVELS

In our survey, the annual rate of growth of fraud was reported as 11% lower than the previous year – still growing, it's important to note, just not at the same breakneck rate.

If the scale of fraud is on the increase, and the barriers to entry are lowered by AI tools, why then did we see a levelling off in the annual growth of fraud?

We have established that new technological adoption by criminals outpaces merchant adoption – for a series of reasons linked to the nature of each pursuit. And herein we find a strong contender for our answer.

It is highly likely that the metrics used by merchants to catalog fraud

are no longer fit for purpose as they are no longer representative of the whole fraud market.

If the KPIs which merchants are monitoring and keeping top of mind are their dispute or chargeback rate, and their decline rate, they may be missing cases of refund abuse rings, voucher fraud, or other more obscure ways to extract value from business systems.

Fraud is a multivariate problem. The industry as a whole is doing a much better job keeping payment fraud under control than when Ravelin first started, 12 years ago, yet struggling with other forms that ecommerce fraud can take.

So while payment fraud, expressed as chargebacks, is perhaps much more controlled today, we believe the true scale of fraud is now underreported by merchants in our and other surveys[1].

We pose this question to the industry: Do chargebacks alone still truly represent the totality of the attack surface? Do chargebacks truly make up the bulk of fraudulent revenue losses? Are complex attacks represented in your chargeback rates?

A COMPLEX, UNDERREPORTED FRAUDSCAPE

In 2026, fraud is more complex than ever. Are merchants aware they're under attack? Is there fraud that's not being detected, happening without the merchant's knowledge?

In this year's survey, we saw refund abuse outrank traditional forms of first-party abuse such as fraudulent chargeback claims in terms of negative impact on businesses. Our respondents also reported that the impact of supplier fraud has increased.

The defenses around conventional payment fraud – authentication, automated defense systems like Ravelin's – are, for the most part, keeping the attackers at bay.

Fraud is an old crime. It was always wishful thinking to expect that attackers would change their ways and start leading a lawful life just because payment fraud became more difficult to perpetrate. They explore new techniques, new attack surfaces, new automation to steal money and data.

We pose this question to the industry: Do chargebacks still truly make up the bulk of fraudulent revenue losses?

And payment fraud has always had a social side beyond the acquisitional nature of the crime. Kudos and clout are currencies in themselves for a cohort of attackers, and the greenfield possibilities of AI mean there is much new territory to be claimed.

INVISIBLE FRAUD & THE NEED FOR NEW KPIS

Therefore, there are areas of activity where fraud is more elusive; where the people getting away with it are all but invisible.

While chargeback rates are tangible evidence of either third- or first-party fraud, it seems that the industry is facing difficulties qualifying and quantifying successful refund abuse – 55% of our respondents are finding this challenging.

When fraud evolves, are we confident that our quantitative understanding of it is fit for

> **Kudos and clout are currencies in themselves for a cohort of attackers, and the greenfield possibilities of AI mean there is much new territory to be claimed.**

purpose?

The ecommerce industry is overdue for developing new, updated metrics to bolster the ones we already use and allow for a more rounded picture of fraud and abuse today.

Payment fraud has a widely acceptable list of metrics that indicate fraud levels.

But payment fraud is no longer our only headache. We ought to come up with new, additional KPIs that we can all agree on that tell us if we're under attack or not.

At Ravelin, we have been thinking long and hard about this and continue to work with merchants to surface metrics that can enhance this understanding.

For example, we look at the total amount of money refunded per customer account and factor into our recommendations its lifetime value (LTV). We also look at the reorder rate following refunds.

Importantly, our survey found that the costs associated with fraud continue to increase, although fraud rates seem to be increasing at a slowed pace. Each year, the typical enterprise incurs losses of $11.4 million, and nearly half of these organizations report that fraud consumes upwards of 1.1% of their annual revenue.

Stopping fraud remains as crucial as ever. As it changes and evolves, we should evolve with it – not only in our technical capabilities but in how we conceptualize and quantify the threat.

THE MERCHANT-CONSUMER RELATIONSHIP IS BEING REDEFINED

We would be remiss to discuss a shifting fraudscape without highlighting the eroding trust between merchant and consumer – a development that would have been hard to predict twelve years ago.

Fraudsters and consumers are no longer seen as markedly different – one group to be blocked at all costs and the other gingerly trusted and happily served.

This is largely down to the willingness of some consumers to treat business policies as disposable or ignorable at their convenience. While this has always existed, the scale of it now is not ignorable by merchants.

The traditional threat model has fundamentally shifted, and the lines continue to dissolve.

This is something that our survey's respondents are painfully aware of. Enterprises are evenly divided on whether it is professional syndicates or their own abusive customers that represent the primary threat to their operations.

And the AI revolution turns up the heat: We have always had first parties attempt limited fraud, such as abusing promotional codes or doing limited multi-accounting, and some businesses cared about this more than others. The potential of AI to industrialize this, however, makes it a pertinent and intensifying pain point for most.

Indeed, the same respondents who reported fraud plateauing still saw an increase in the likelihood that first parties will attempt abuse.

Whether as a result of financial pressure, inflation or even peer pressure, there is increasing evidence[2] that everyday consumers are more likely to attempt to circumvent merchant policies.

ERODING TRUST & A LACK OF CONFIDENCE

Moreover, the findings highlight a lack of confidence in merchants' understanding of their customer base:

On the one hand, merchants are not certain they can tell when their customers are taking advantage of them. For instance, 6 in 10 are not confident identifying legitimate refund requests from fraudulent ones.

On the other hand, there is confusion surrounding whether robust fraud defenses have a positive or negative impact on merchants' customer base: Merchants report customer friction as the main obstacle to improved fraud detection, yet at the same time believe media reports of fraud erode customer loyalty (77%) and consumer trust (81%) in their company.

In the age of social media, consumers have megaphones that can significantly impact a company's public image. False positives and "customer insults" have potential for a wider detrimental effect than they used to.

> **The ecommerce industry is overdue for developing new metrics to bolster the ones we already use and allow for a more rounded picture of fraud today.**

It is from there that we come to one of the most evergreen questions in fraud detection: friction. What should a merchant do? The answer remains opaque to many.

That merchants hesitate to be more decisive with fraud for fear of introducing friction signals a level of uncertainty in decisioning which may hinder efficiency and increase risk.

WHERE DO WE GO FROM HERE?

Fraud detection should be both a tool and an enabler of your strategy. When deployed correctly and as part of a cohesive, holistic fraud strategy, anti-fraud software can only have a positive impact on your business, including on the customer experience. Customers still have appetite to know their data is being protected, and that they're dealing with a merchant sensitive to the problem of fraud.

If you are concerned that your fraud defenses negatively affect your customers – be that through false positives, friction or otherwise – make sure you raise

> **There is confusion around whether robust fraud defenses have a positive or negative impact on merchants' customer base.**

> **As fraud changes and evolves, we should evolve with it – not only in our technical capabilities but in how we conceptualize and quantify the threat.**

this with your fraud detection vendor.

Questions around friction, customer journeys and public perception are a healthy path to reaching the answers that work for your organization.

Ultimately, the best response is customized to every business.

A great anti-fraud vendor will take into account your company's requirements and goals, and help you craft a strategy that does not add friction for good customers, instead unlocking opportunities to cultivate loyalty in those who do not attempt fraud nor abuse your policies.

At Ravelin, we are proud to enable secure growth for our merchants – not simply stopping fraud but building better experiences for their customers. ■

4+ billion
transactions per year

$62 billion
in transactions processed

340+
merchants protected

Ravelin

METHODOLOGY

In January 2026, Ravelin commissioned research provider Qualtrics to carry out an online survey of **1504** fraud and payments professionals from around the world, with a focus on the UK, USA, Canada, France, Germany, Italy, Spain, Australia, Brazil, and Mexico.

Participants belonged to the C-suite or Fraud/Risk, Finance/Payments, Compliance/Operations or Product teams of enterprises in the following industries: Online Retail, Travel, Transport & Hospitality, Digital Goods & Subscriptions, Online Marketplaces. Enterprises were defined as businesses with more than $50 million in annual revenue and/or over 500 employees, which sell their products either online or both online and offline.

They were asked questions around their observations, attitudes and predictions related to fraud, payments and ecommerce in the past 12 months, at present, as well as in the future.

All 2025 data referenced is from Ravelin's Global Fraud Trends: Fraud & Payments Survey 2025. All 2024 data referenced is from Ravelin's Global Fraud Trends: Fraud & Payments Survey 2024.

REFERENCES

1 https://merchantriskcouncil.org/learning/mrc-exclusive-reports/global-payments-and-fraud-report

2 https://pages.ravelin.com/refund-abuse-trends-report-2026-survey


Canada
USA
Mexico
Brazil
UK
Germany
Spain
France
Italy
Australia

RAVELIN

Thank you for reading our Global Fraud Trends Report

Ravelin has built solutions to address all these pain points, learning from your historical data to inform an AI-native fraud prevention strategy that works for your specific landscape – and no-one else's.

Get in touch today to chat about payment fraud, account takeover attacks, refund abuse, voucher, promo & policy abuse, transaction optimization, 3D Secure, link analysis or supplier fraud.

Book a call at ravelin.com/contact-us.

Questions? Comments?
Please write to marketing@ravelin.com.

We frequently release new findings in fraud and payments.

Make sure you follow us on LinkedIn or by signing up at ravelin.com.

V1.0