Ravelin

RETAIL ECOMMERCE

FRAUD & PAYMENTS SURVEY

ravelin.com

CONTENTS

CHAPTER		PAGE
1.0	Introduction	3
2.0	The Covid-19 effect The pandemic's impact on retail businesses, ecommerce and fraud teams	4
3.0	Retail fraud teams Size, growth predictions, department and wider business perception	8
4.0	Tools & budgets Fraud team budget forecasts and tools used against fraud (in-house vs. outsourced)	14
5.0	Fraud trends & top risks 12 month increases in top fraud risks and rising trends	19
6.0	Monitoring fraud Factors used to identify/track fraud, and time spent on manual review	24
7.0	Chargeback management Challenge and success rates	28
8.0	Account takeover Retail vertical differences and reporting attacks	30
9.0	Payments Monitoring fraud by payment methods and current 3D Secure transactions	34
10.0	Europe's PSD2 legislation Perceptions, readiness and awareness of PSD2 post-Brexit, comparing the UK, Europe and US	38
11.0	Summary	40

1.0 INTRODUCTION

Last year was turbulent for retail merchants, as brick-and-mortar sellers were forced online and ecommerce transaction volumes reached new heights. In early 2021, Covid-19 is still at large, driving retailers to focus on how to make remote and contactless operations work long-term. With the final PSD2 deadline approaching, retailers should expect more challenges ahead.

Retail businesses are hot targets for fraud, as cases of online payment fraud and account takeover (ATO) increase, and risks from genuine customers emerge, such as a rise in refund abuse. Are retail fraud operations agile enough to withstand the challenges this year will bring? Our findings highlight the areas where retail merchants need to adapt and optimize in their online security to stay safe in 2021.

This report provides insights into:

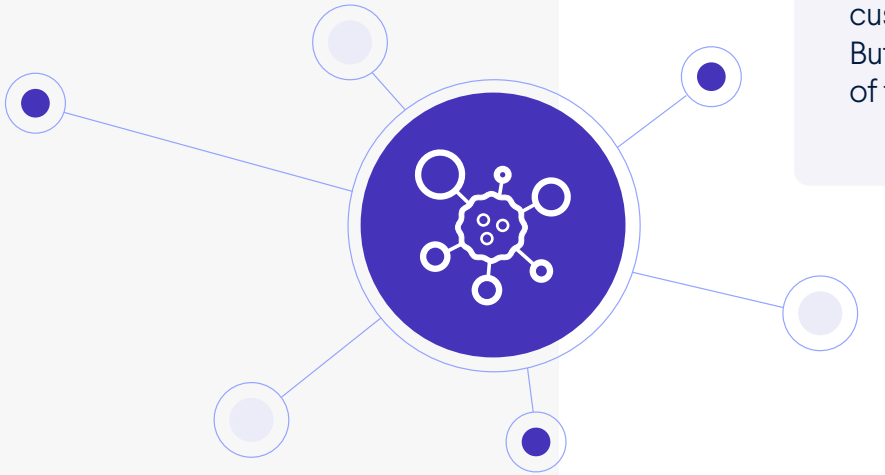
- Merchant perceptions of how fraud is changing and top business threats
- Tools, budgets and methods for monitoring fraud and false positives
- The macro environment impact, including Covid-19 and PSD2
- Survey methodology

Survey methodology

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

2.0 THE COVID-19 EFFECT

In 2020, the Covid-19 pandemic took hold, disrupting business operations worldwide. Almost a year later the crisis continues - with **50 countries still completely closed, and 121 only partially open (Feb 2021)**. Within countries, internal restrictions on movement are bringing customers online and accelerating the digital shift for retail merchants.



Last year was record-breaking for retail ecommerce. The UK Domain monitored 2020's online traffic and found that more retailers made the top 100 websites list than ever before. Fashion retailer ASOS saw its UK website traffic increase by 62 million visits and interior-design retailers made their list debut.

With increased ecommerce and in times of crisis, **online fraud risks grow**. Amid a looming global recession, there's a higher risk of opportunistic fraud from genuine customers under increased financial strain. But how do retail merchants see the impact of the pandemic on their business?

Over half of retail merchants see Covid-19 as positive for fraud team operations

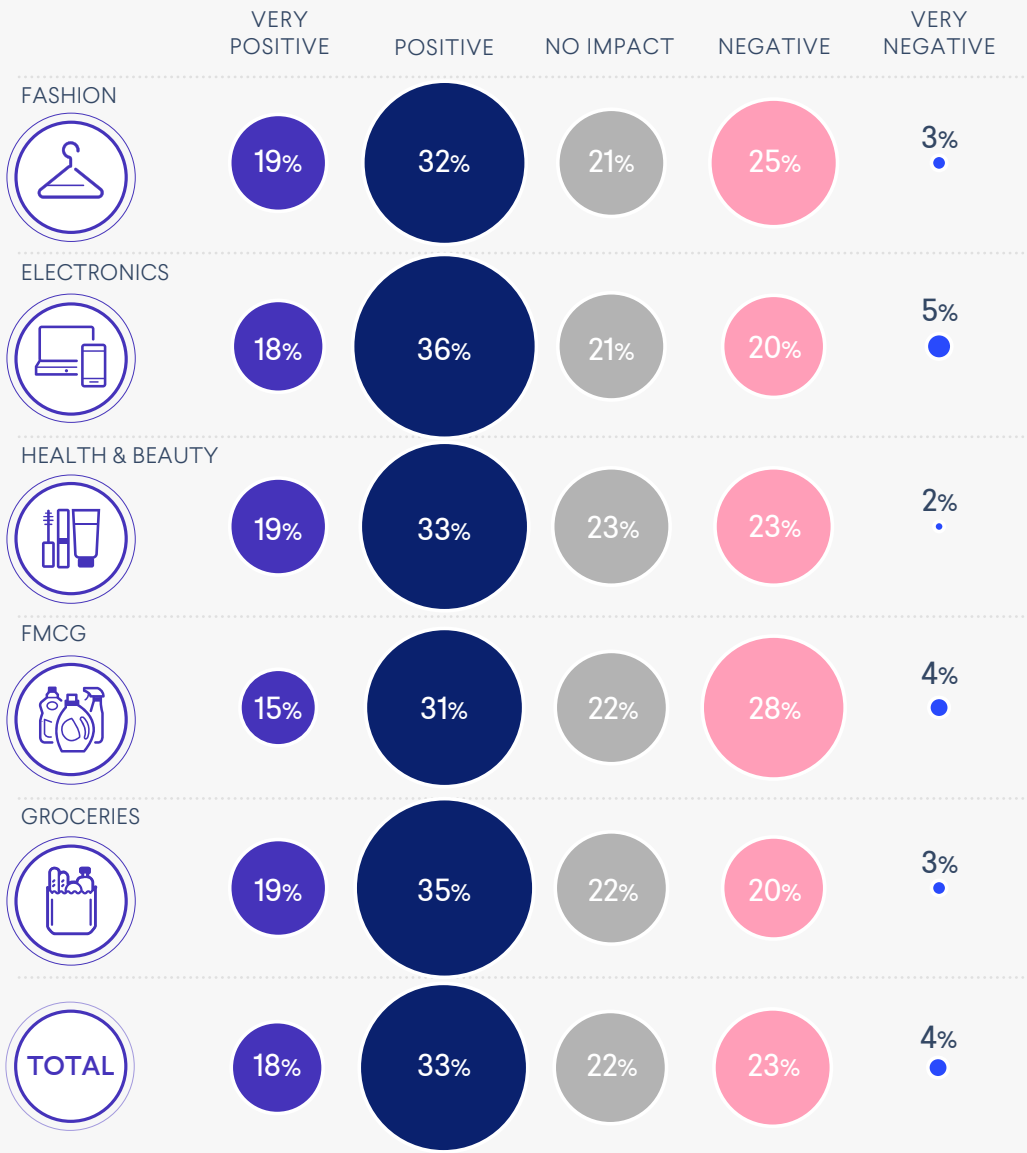
In our wider study across four industry groups (Retail, Digital goods, Travel & Hospitality and Marketplace) an average of 46% of businesses said the Covid 19 pandemic had a positive impact on their fraud operations.

For retail merchants, this is higher with an average of 51% saying the pandemic has had a positive impact on their business fraud operations. Within the retail merchants, electronics and groceries retail merchants are more likely to see the pandemic as a positive. These two retail sectors have seen a boom in online sales due to the pandemic, as consumers work, play and order their groceries from home.

51%

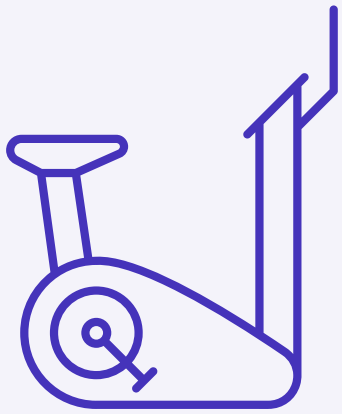
51% of retailers say the pandemic had either a positive or very positive impact on their business fraud operations

IMPACT OF COVID 19 ON **RETAIL INDUSTRIES**



A new way of life requires new gadgets

The pandemic has turned daily routines upside-down for families, students and professionals. Adjusting to the new normal led **consumers to buy previously unpopular gadgets** relating to **at-home learning, remote work, health and entertainment.** For example, fitness exercise machine manufacturer Peloton said Covid-19 **'changed everything' and saw their rapidly growing business explode even further.** The massive growth in demand from genuine customers outstripped fraud, as recorded by checkout platform Bolt in their **Covid-19 Impact Report.**



Pandemic impact is more positive for online grocery merchants in the UK than in the US

With many restaurants and eateries forced to close, groceries sales rocketed. In one week in March 2020, UK supermarkets recorded a whopping **15 million** visits from customers, with **groceries representing over half of all retail sales.**

How does the impact of Covid-19 differ for grocers in the UK vs. the US?

It's interesting to note that UK groceries merchants are more likely to perceive the pandemic as having a positive impact on fraud operations. This may be partly due to the fact the UK grocery market has a strong online presence, **with over a third of UK customers buying their food shop online even before the pandemic.** As a geographically small country, UK grocery merchants can perform online deliveries easily, with more stores close to homes.

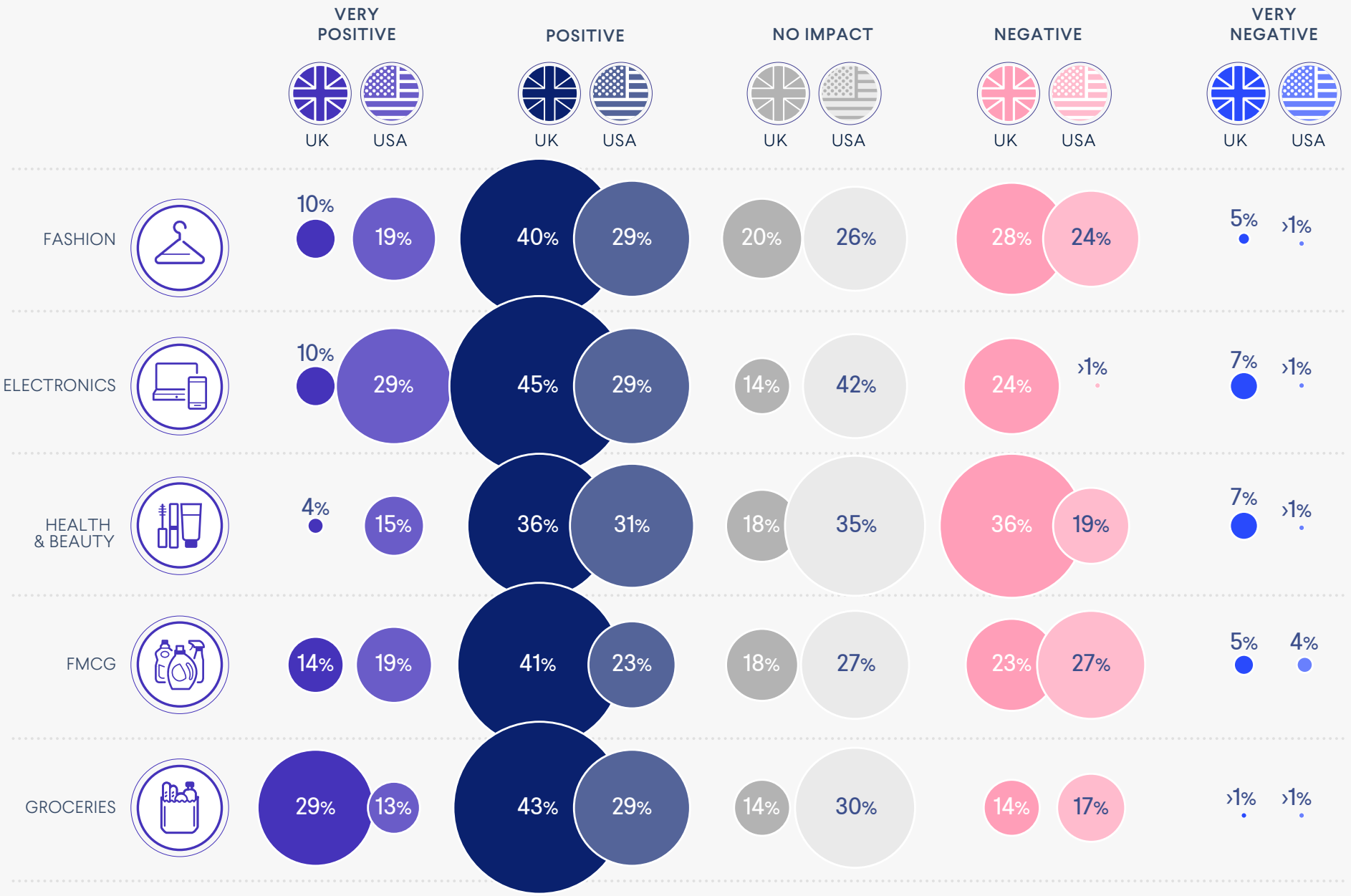
During the first wave of Covid-19 in 2020, UK groceries were stretched by demand to such an extent that **many grocery stores restricted online orders to existing customers only, including Sainsburys and Ocado.** Selling only to their known and trusted customers massively reduced the fraud rate for many online grocers, while sales went up.

The vastness of the US makes grocery deliveries more difficult, with populations spread out, and with more rural communities. Whilst **US grocery sales jumped 300% early in the pandemic**, merchants and customers have not embraced deliveries to the same extent as the UK. Therefore, US grocers would not have had as much of a notable reduction in fraud through online channels.

72%  Vs **42%** 

Grocery merchants perceive the pandemic as having a positive or very positive impact on fraud team operations

IMPACT OF COVID 19 ON **RETAIL INDUSTRIES**



3.0
RETAIL FRAUD TEAMS

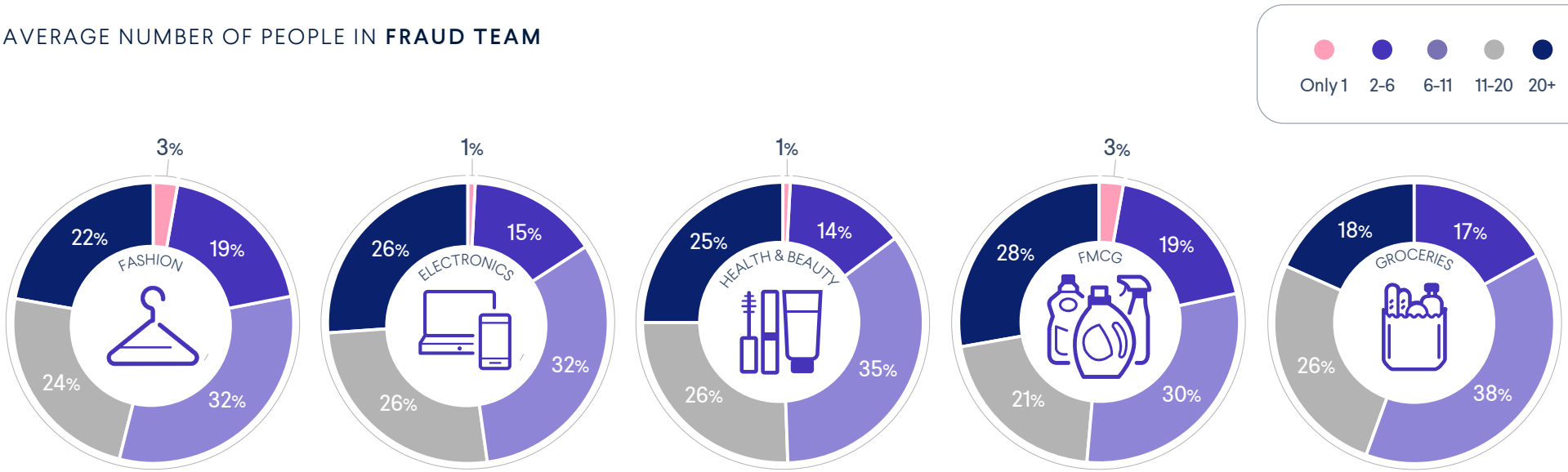
The size of the retail fraud team

Retail fraud teams are likely to be larger than other industries, as shown in our wider survey results. Within retail, 48% of merchants have a fraud team of 11+, with even higher percentages for electronics, health & beauty, and FMCG merchants.

48%

48% of retail merchants have fraud team of 11+

AVERAGE NUMBER OF PEOPLE IN **FRAUD TEAM**



High-value electronics merchants have the biggest fraud teams

Over half (52%) of electronics merchants have fraud teams of 11-20+ people. Electronics merchants tend to sell high-value merchandise that can be easily shipped and resold, making them popular fraud targets. With high-value products at stake with every successful fraud attack, electronics retailers may be more sensitive to fraud risks.

52% of electronics merchants have fraud teams of 11-20+ people

Almost a quarter of fashion and FMCG fraud teams have five people or less

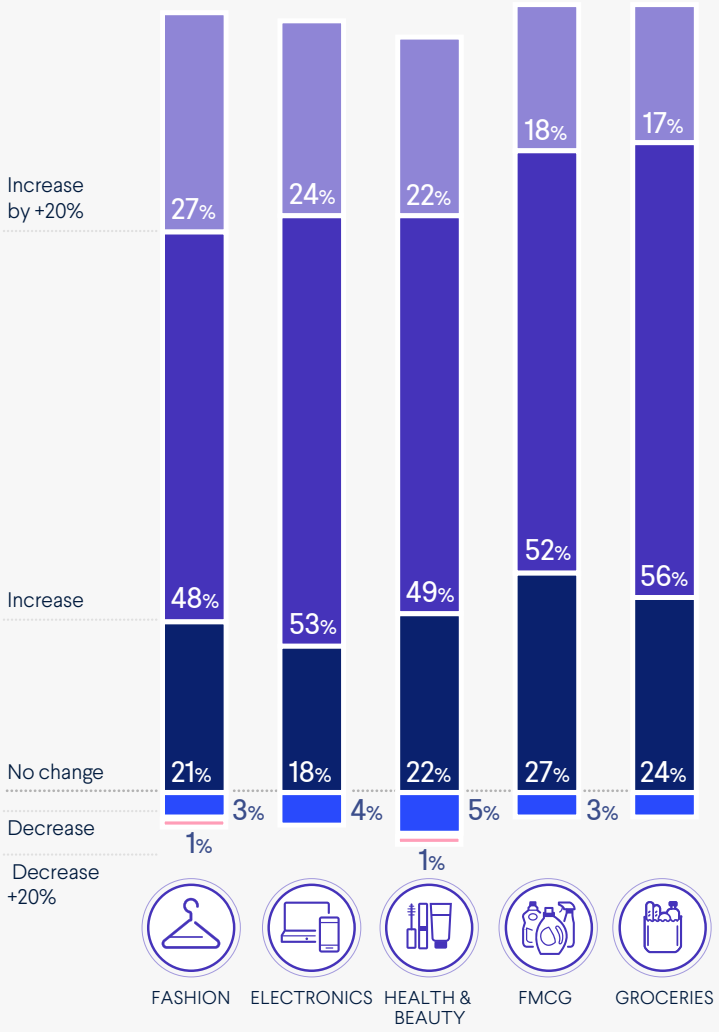
Fashion and FMCG merchants tend to have smaller fraud teams, as 22% of both have teams of under five people, (above the retail survey average of 18%).

FMCG merchants rely on selling large volumes of low-cost products, therefore they may have a more lenient view to fraud risks compared to higher value electronics retailers. This can also be true of fashion retailers, but as we will learn later in the survey, fashion fraud teams are both small and potentially overloaded with responsibility, from large amounts of manual review work to chargeback management. A spike in fraud would cause serious issues for fraud teams in these industries if they don't have the right tools to protect their business.

22% of fashion merchants tend to have fraud teams of under 5 people

Fraud team growth predictions

Retailers are looking to invest in fraud management despite business uncertainty, with an average of 72% expecting the fraud team to grow in the next year.



More electronics and fashion retailers are expecting to increase fraud team size

More fashion (75%) and electronics merchants (77%) are expecting their fraud teams to increase. This could be a reaction to fraud risks growing, as teams must expand to keep up. As fashion retailers are more likely to have smaller fraud teams, it's promising they have the biggest vote for expecting 'significant increase' at 27%.

The most electronics retailers, 77%, are expecting an increase, even though they already tend to have larger fraud teams. This might be due to the consumer boom in electronics seen in 2020 combined with the higher value of electronics orders.

Quality over quantity can apply to fraud teams, and business-leaders should equally invest in empowering their existing team with more effective tooling and enabling them to upskill.

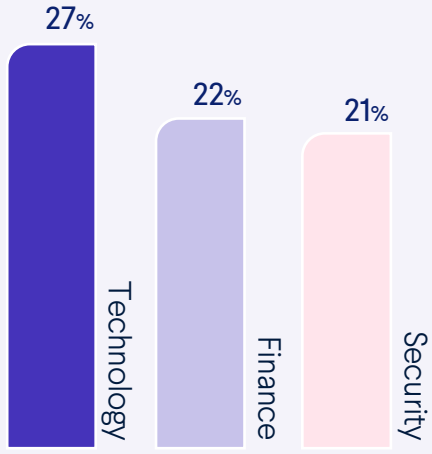
3.1 RETAIL FRAUD TEAMS

Business department

As fraud teams are multidisciplinary by nature, there doesn't seem to be a single department where retail fraud teams sit. Additionally, the fraud team position within the business is also impacted by the business growth strategy and market position.

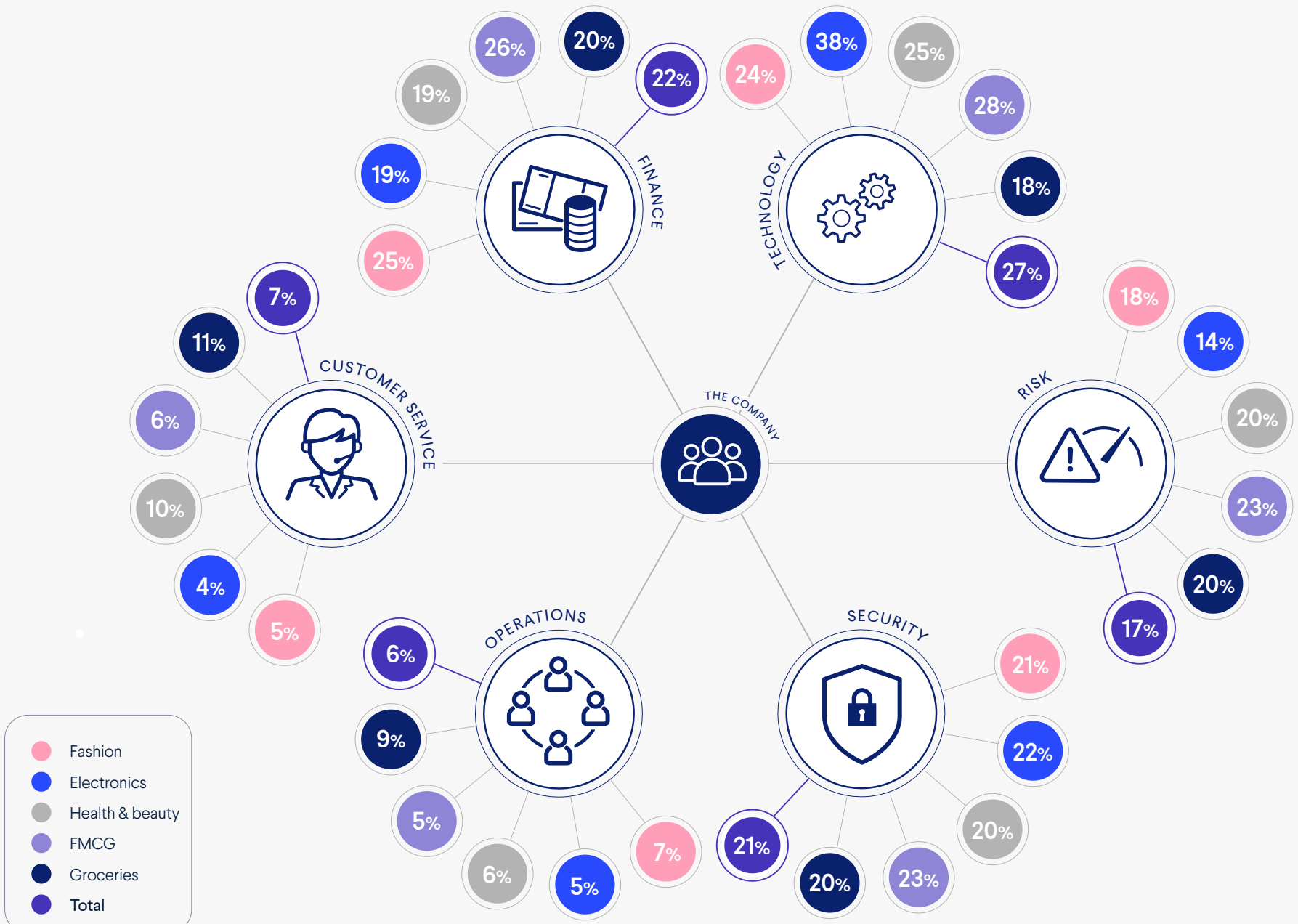
On average, over a quarter of retail fraud teams (27%) sit in the technology department, closely followed by finance (22%) and security (21%). The high proportion of retail fraud teams in technology could reflect the increasing importance of ecommerce, which is likely to develop further.

Electronics retailer fraud teams are the most likely to sit in the technology sector. Perhaps these fraud teams are more technologically specialised and mature, as well as being larger.



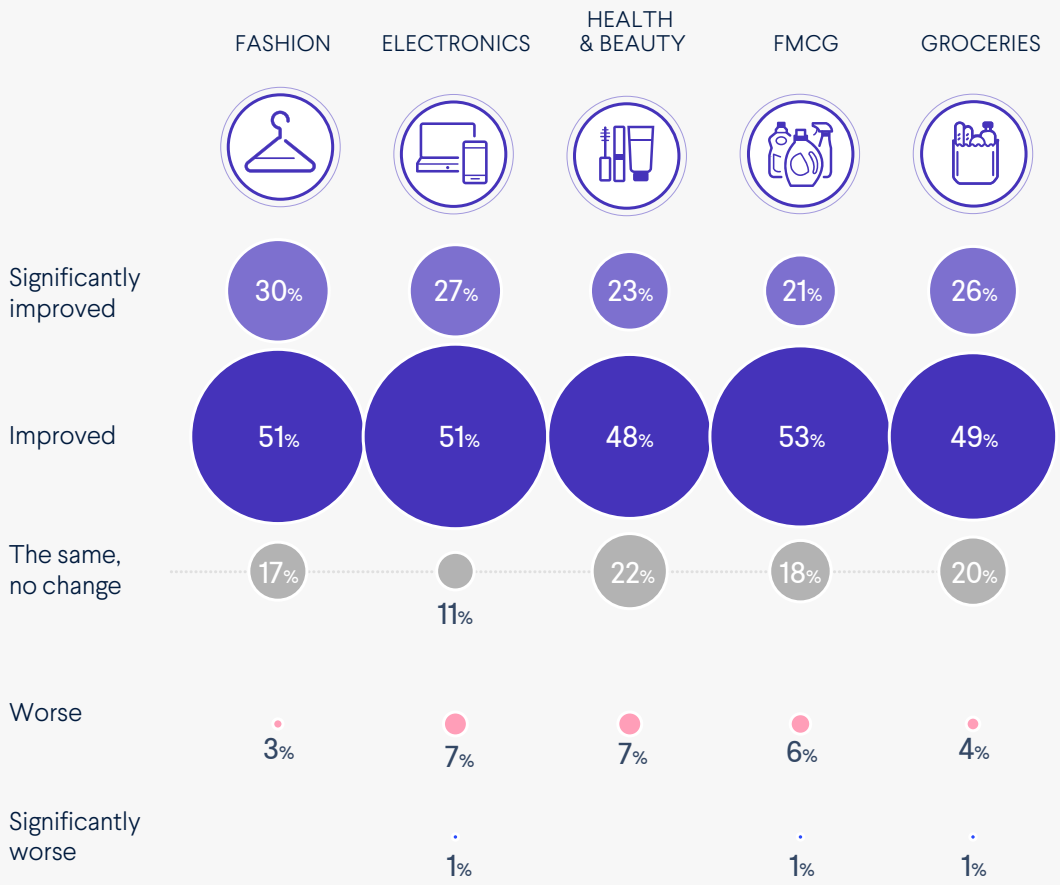
Retail fraud teams

FRAUD TEAM DEPARTMENT **WITHIN THE BUSINESS**



3.2 RETAIL FRAUD TEAMS

Business perception of the fraud team



Over three quarters (76%) of retail merchants have noticed an improvement in the wider business perception of the fraud team in the past 12 months.

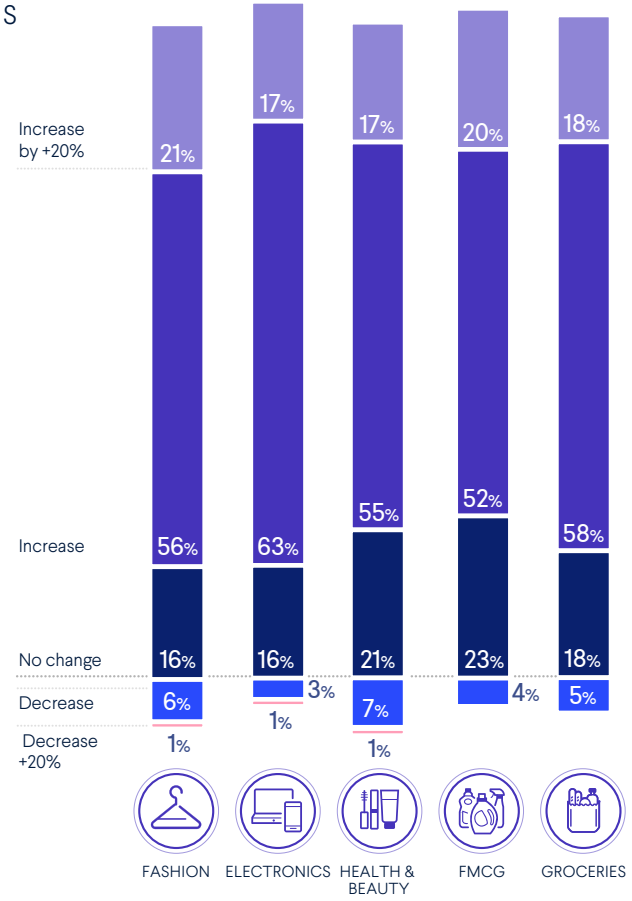
Traditionally the fraud team is stigmatized by other business teams, seen as a blocker of sales or thought to hinder growth. **In our recent webinar, Krystyna Savotchenko discusses having to "fight the perception that fraud prevention damages business"** and educate other departments on the importance of fraud protection. Some merchants have revealed that renaming the fraud team 'Risk' or 'Revenue Assurance' can significantly improve wider business perceptions. Retail fraud teams may have to work harder to debunk this myth more than other industries, as retailers prioritise fast sales and frictionless customer experience above all else.

A large proportion of fashion retailers have seen a boost in fraud team perception (81%), perhaps due to accelerated technological development over the past year, accelerated by Covid-19. It is positive that fraud teams are gaining respect from C-level (43% of survey participants).

4.0
TOOLS & BUDGETS

Fraud budget forecast in the next 12 months

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



76%

76% of retail merchants predict their budget to tackle fraud will increase in the next 12 months

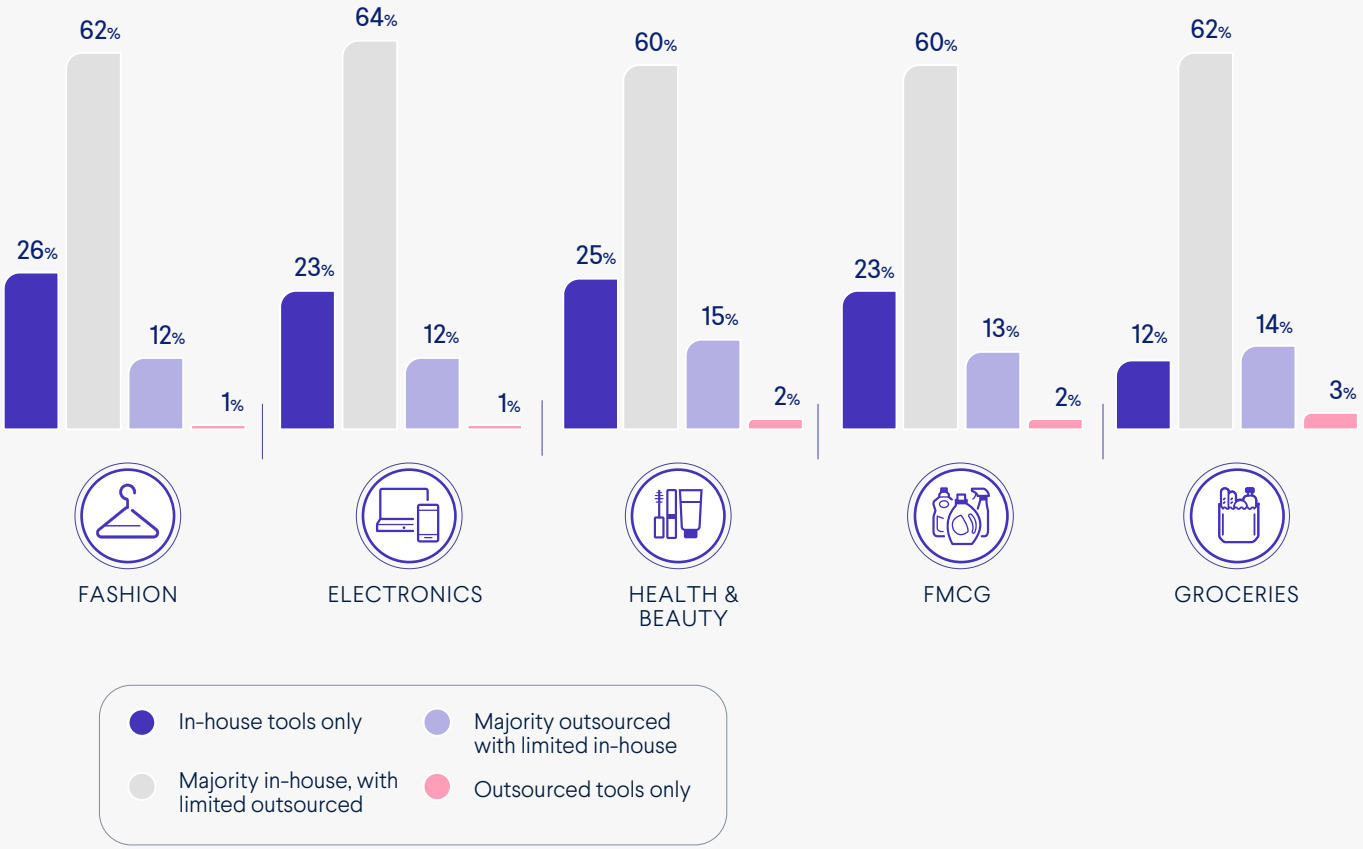
Overall, 76% of retail merchants predict their budget to tackle fraud will increase in the next 12 months, with 20% anticipating a significant increase. Retailers are starting to arm themselves against fraud, correlating with businesses reporting a rise in multiple fraud-types.

One-fifth of retailers are expecting a significant increase in fraud budget

There is a direct correlation between an increasing fraud budget and the expectation of growing the size of the fraud team. Of all survey-participants who predicted a significant increase in their budget, 95% also predicted an increase in fraud team size.

4.1 TOOLS & BUDGETS

Tools used against fraud

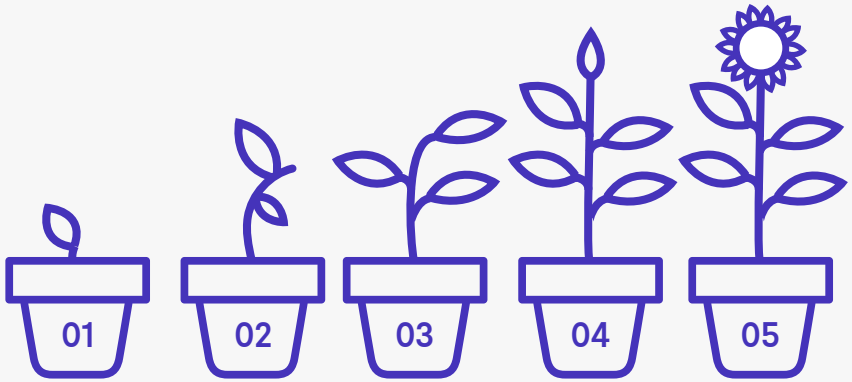


Three quarters of retailers (75%) are using a mixture of in-house and outsourced tools against fraud. Whilst this is the majority, it is less than the survey average of 79%, suggesting that retailer's fraud priorities differ.

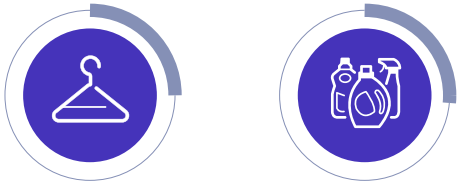
The right fraud tools can depend on your business growth stage
Florian Jensen - Glovo

In our merchant survey webinar, Florian Jensen from Glovo explains how and why the fraud tools a merchant uses can depend on the stage of growth of the business. Growing businesses can use static rule systems to fight fires and learn about their customers. But as fraudsters learn how to mimic genuine customers, rules can become insufficient.

Adding machine learning to your toolbox can help reduce the repetitive work for the fraud team and streamline operations to give you the best of both worlds.



Growth stages



25% **26%**

Use in-house tools only

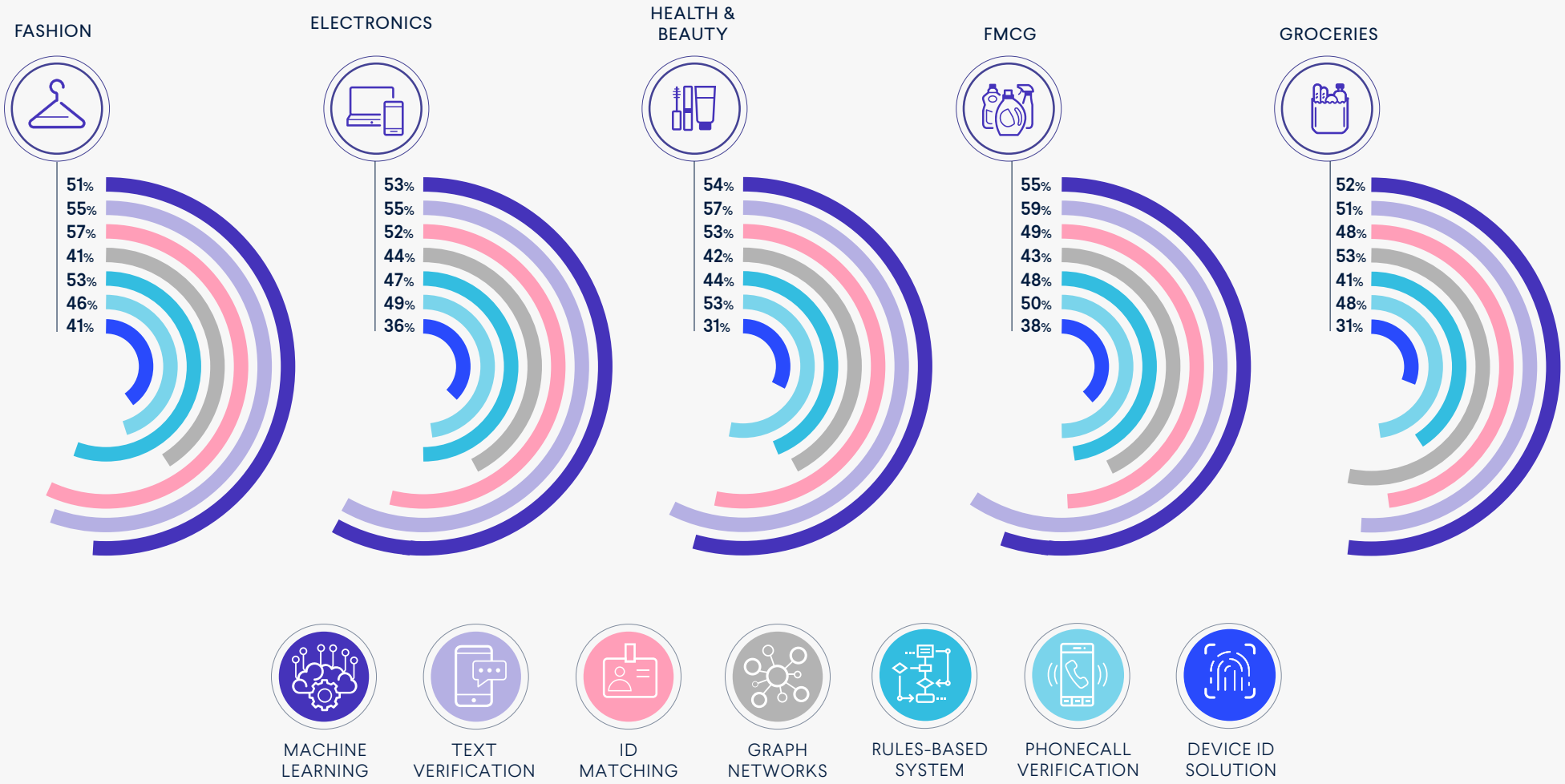
Over a quarter of fashion retailers use in-house tools only

Over a quarter of fashion retailers (26%) use in-house tools only, which is surprisingly high since they are more likely to have small fraud teams. Similarly, 25% of FMCG use in-house tools only and also tend to have smaller fraud teams.

Whilst in-house tools can be effective, designed according to specific business needs, they are usually rules-based, and often aren't as agile as machine learning. It's definitely possible for merchants to develop machine learning models in-house, but it **requires significant investment from the business** and so it's rare to find merchants who choose to do so.

Machine learning used less widely in retail compared with other industries

TOOLS USED TO **TACKLE FRAUD**



On average, 53% of retail merchants are using machine learning, compared with 58% for both travel and marketplace merchants and 60% for digital goods merchants.

Many retail businesses have a combination of in-store sales and online sales, and therefore online fraud may have been seen as less critical. However, as more and more customers now choose online, further amplified by the pandemic, retail merchants will pay more attention to online sales and seek to minimize fraud loss online too.

More fashion merchants use rules-based systems (53%) over machine learning models (51%) which is another indication that fashion fraud teams are perhaps behind the curve with regards to fraud defence. In general, retail merchants are also more likely to use rules-based systems than other industry merchant groups, perhaps reflecting the limited investment in online fraud protection so far. Machine learning models adapt and learn when given more data, and so they can be incredibly effective for constantly-changing retail businesses with high order volumes.

Text verification is the retailer's favourite tool

Text verification is the most popular fraud tool for retailers, used by over half retail merchants (55%). Health & beauty (57%) and FMCG retailers (59%) are most likely to use text verification tools. In our broader survey including other merchant industries this was the second most popular tool among travel, digital goods and marketplace merchants after machine learning.

Fewer retail merchants use graph network and and device ID tools in the face of growing account takeover threat

Graph networks are used by 44% of retailers, the lowest of merchant industries we surveyed. The same goes for device ID, as the least used tool for retail merchants (36%). Retail's lower use of these tools is a concern in the face of growing ATO threats. Almost half of all retail merchants experienced a rise in ATO activity and on average suffered 33 high impact ATO attacks in the past year. Network analysis and device ID tracking are critical methods for detecting and stopping account takeovers.

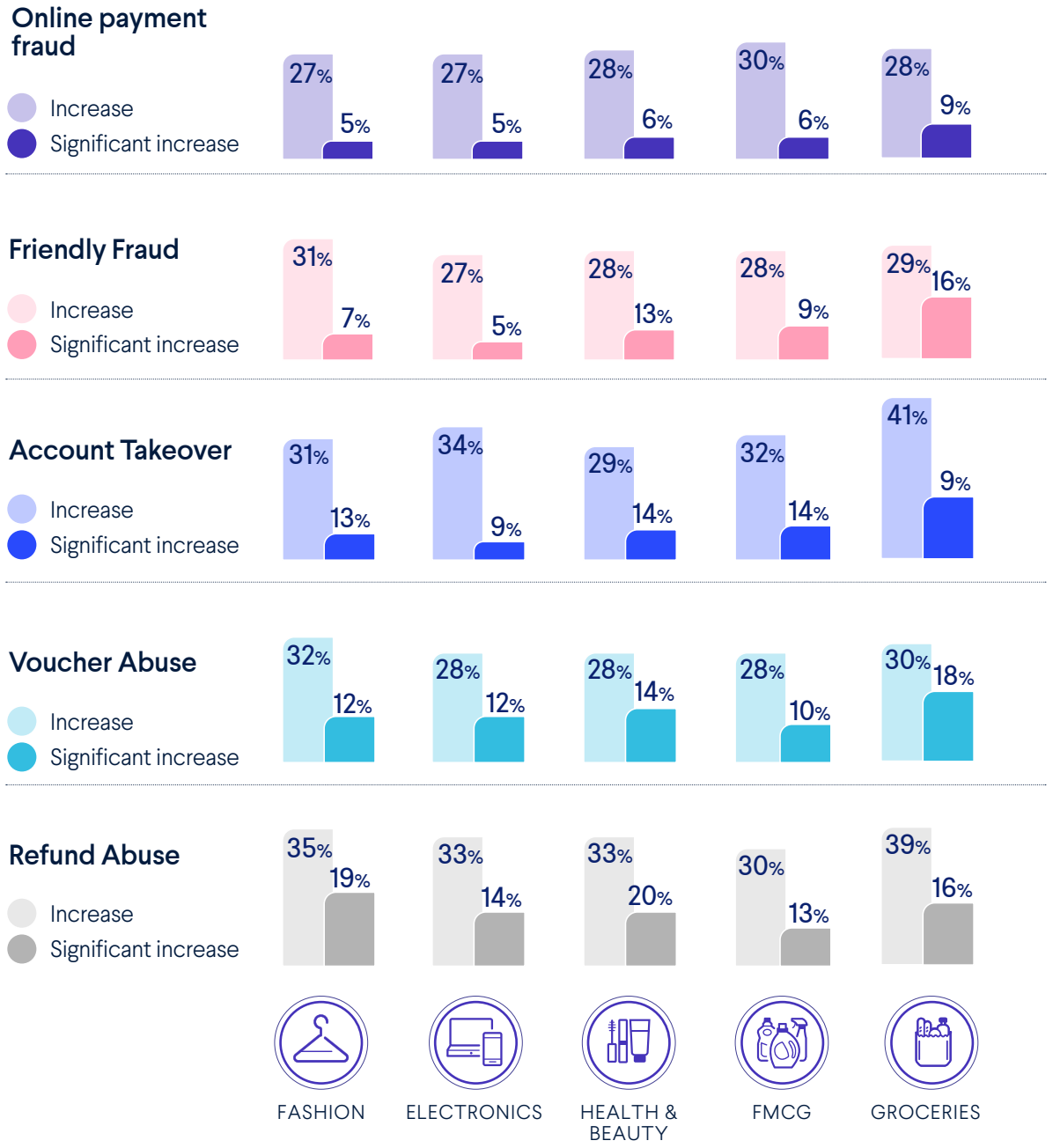
5.0 FRAUD TRENDS AND TOP RISKS

Fraud is increasing against retail merchants

For retailers, refund abuse and voucher abuse are surging and attracting the attention of C-level, no longer accepted as an inevitable cost of doing business.

On average, grocery merchants are more likely to see an increase in most forms of fraud. For example, 45% of all retail merchants have seen an increase in ATO, for grocery merchants this figure is 50%.

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



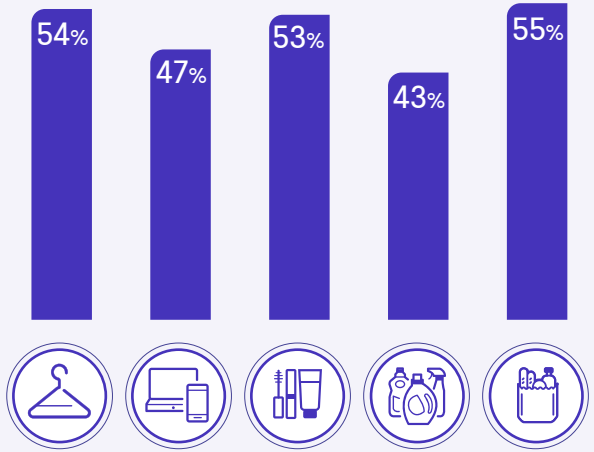
Refund abuse increased most for groceries and fashion retailers

Refund abuse has increased for half (50%) of retail merchants in the past 12 months. Fashion (54%) and grocery (55%) merchants saw refund abuse increase the most, with FMCG (43%) and electronics (47%) less likely to see an increase.

Fashion retailers may have been impacted by the pandemic preventing shoppers from trying clothes on in store, and returning more items than usual. **Wardrobing and social media 'refund hacks' have gained popularity**, affecting fashion merchants. **Extended refund periods** and huge returns chains mean more strapped for cash customers try their luck with refunds.

The pandemic has also stretched grocery retailer operations to the limit, with customers complaining on social channels about deliveries being delayed or cancelled or missing items. **Customers can request refunds on groceries orders** if items are short in their 'use by' dates, missing or damaged in transit. Opportunistic customers are aware that these complaints are hard to discredit, especially with socially-distanced delivery, and can easily take advantage.

Refund abuse has increased for 50% of retail merchants

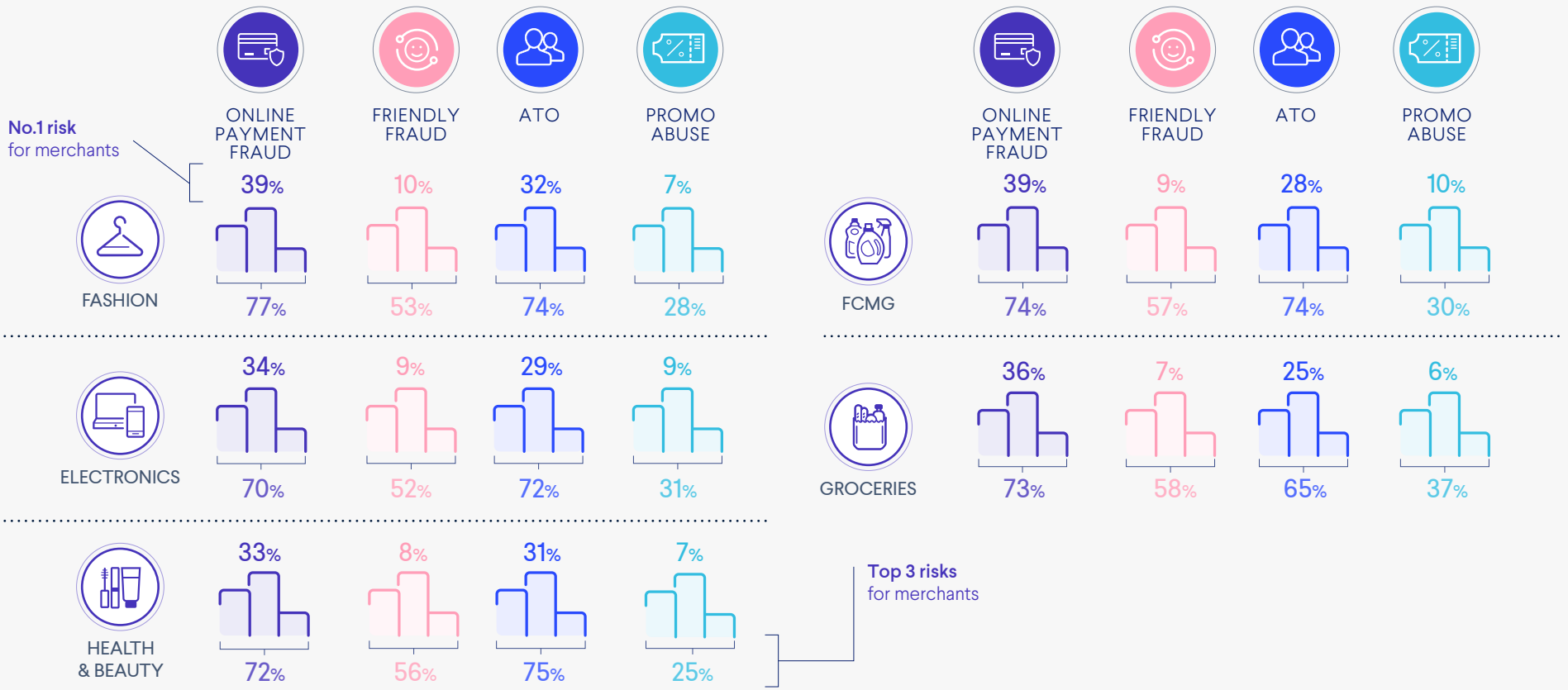


Increase in refund abuse in the past 12 months

5.1
FRAUD TRENDS AND TOP RISKS

Top fraud risks

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



Online payment fraud is perceived to be the biggest risk

We asked merchants to rank fraud types in order of the risk to their business. The majority of retail merchants see online payment fraud as their number one business risk. Online payment fraud is a constant challenge. Despite some industries bentefiting from reduced fraud due to the global pandemic, it is still the most costly and tangible fraud against merchants. A recent study by Juniper finds that **eCommerce merchant losses to online payment fraud will exceed $25 billion in 2024.**

Almost 40% of Fashion and FMCG merchants see online payment fraud as their biggest fraud risk. This may be due to merchants in these sectors having smaller margins on products and being reliant on larger order volumes.

40%

Online payment fraud is seen as the biggest fraud risk to 40% of Fashion and FMCG merchants

Retail merchants recognize ATO as a significant risk

Overall, 72% of retail merchants see ATO as one of the top three threats to their business. In fact, both health and beauty and electronics merchants are more likely to have ATO in the top three risks than any other fraud type, including online payment fraud. According to this metric, it's seen as the same level of risk as online payment fraud for FMCG merchants.

ATO is far more challenging to measure accurately than online payment fraud. Although there may be chargebacks associated with ATO, it's also hugely damaging to a brand reputation when an attack affects a large proportion of users. The damage is amplified if merchants don't have robust operations and processes to reassure and solve customer enquiries fast after an attack. In highly congested and competitive retail markets, brand reputation and customer loyalty is critical – particularly in industries where customers frequently reorder from the same brands, such as health and beauty.

Groceries merchants are less likely to see ATO as one of their top three fraud risks – despite half reporting an increase in ATO activity. It may be that grocery merchants underestimate the risks associated with ATO as it's more unusual for customers to order groceries to many different addresses, and this would be quickly flagged as suspicious. Although **most ATO attacks result in the fraudster placing an order**, fraudsters can also steal customer details - so it is still important to protect against ATO.

72%

ATO is seen as a top three threat by 72% of retail merchants

Fewer retailers see promotion abuse as a top threat

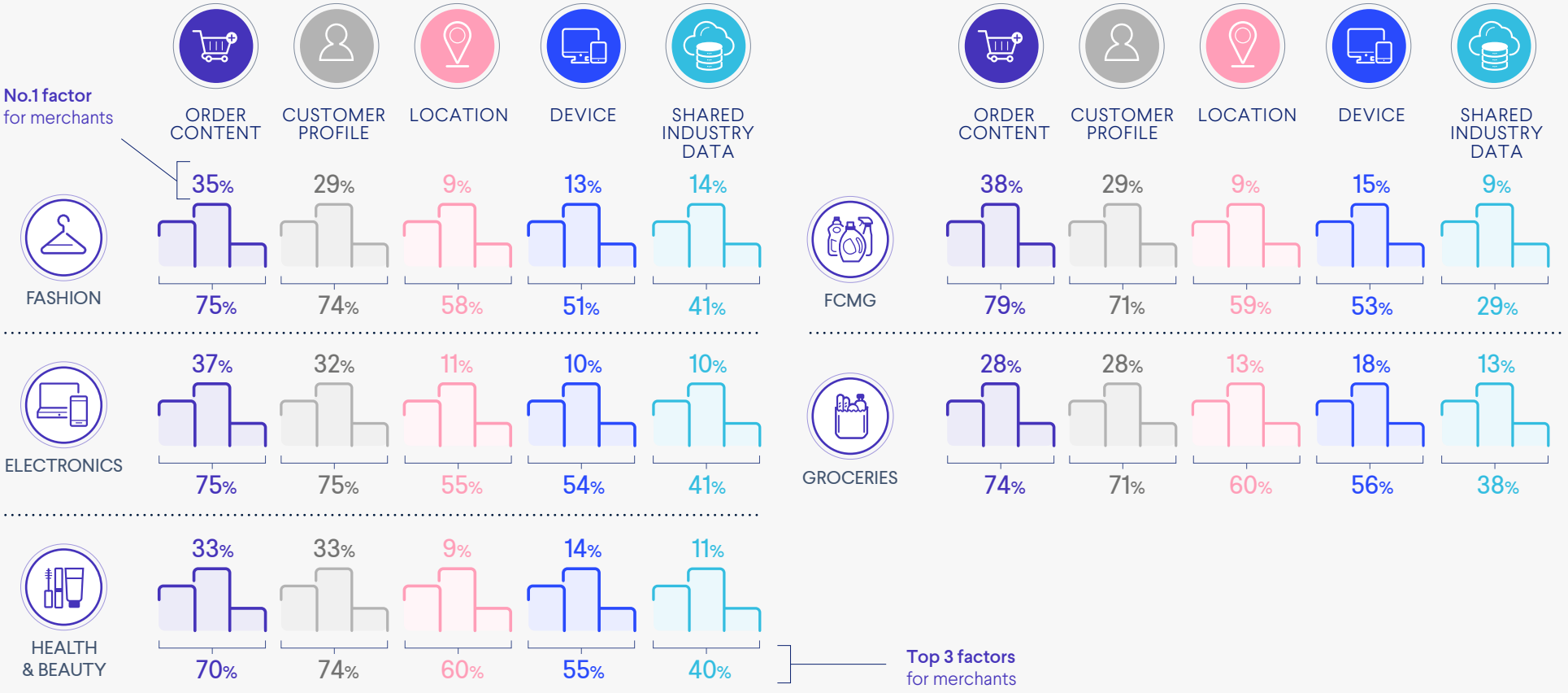
Fewer retail merchants see promotion abuse as one of the top business risks, despite seeing large increases in promotion abuse activity. Overall, 30% of retail merchants see promotion abuse as a top concern, compared with 38% of digital goods merchants, 37% of travel merchants and 32% of marketplaces. This could be an indication that retailers have come to accept promotion abuse as the cost of doing business - or perhaps they are more confident in their strategy to manage the risk than other industries.

Within retail, groceries merchants are most likely to see promotion abuse as one of the top threats to their business, which may reflect the trend for groceries merchants to offer large discounts for new customers.

6.0 MONITORING FRAUD

We asked merchants about what they see as the key factors to identify fraud.

TOP FACTORS TO IDENTIFY FRAUD



Order content is the no.1 key fraud indicator for all retail verticals

Order content is more important to retail businesses than other industries - 34% of retail merchants see order content as the most important factor compared with 30% of travel and marketplace merchants and 24% of digital goods merchants. This reflects the nature of retail, as fraud teams of consumer goods businesses can flag very high value orders, bulk orders or typically risky items like expensive alcohol.

A third of health and beauty merchants see the customer profile as the number one factor to identify fraud

As with other industries we surveyed in our larger report, fewer retail merchants see shared industry data as a critical indicator of fraud.

74%

Three-quarters of retail merchants see customer profile as a key fraud indicator

6.1 MONITORING FRAUD

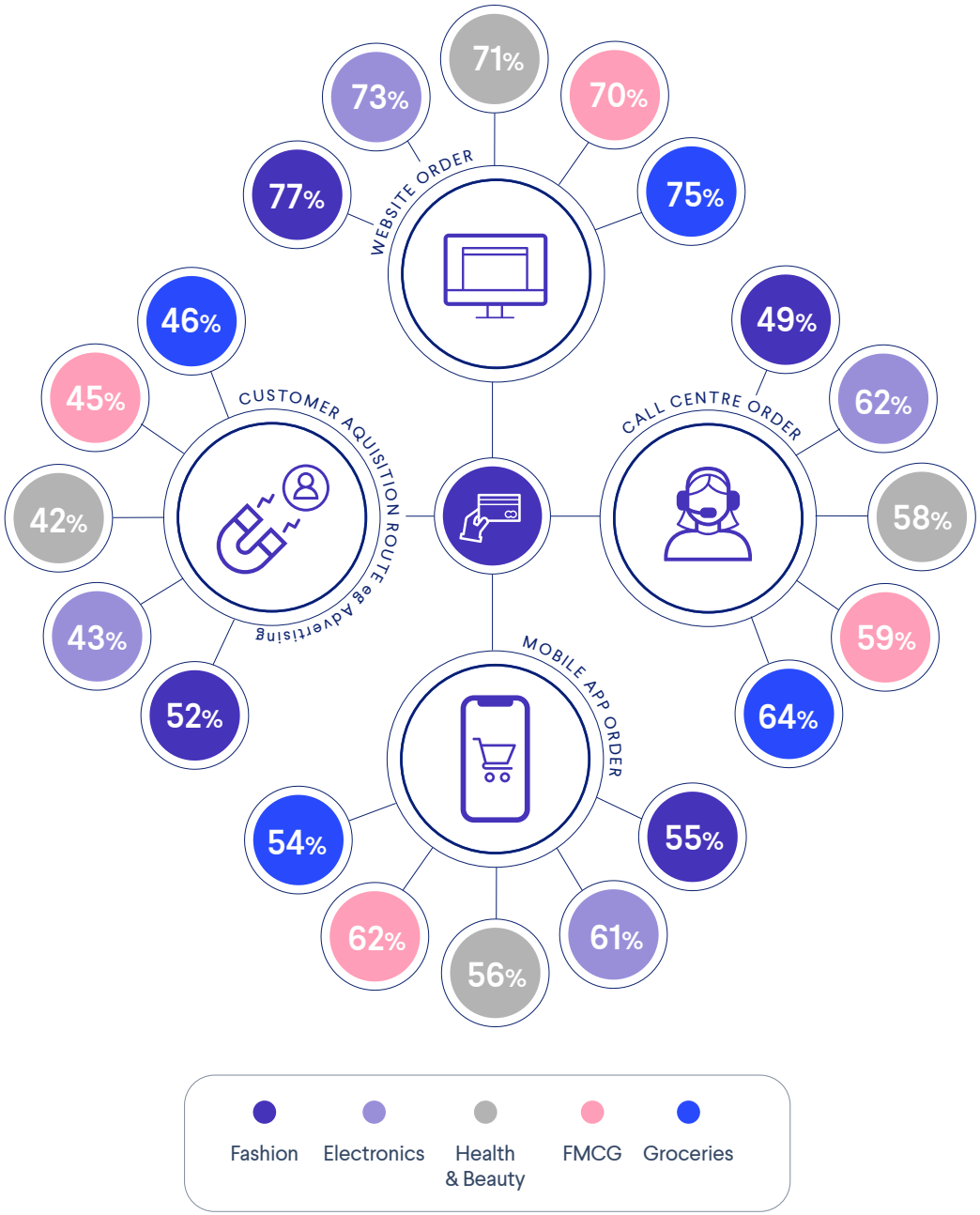
Tracking fraud by customer journey

Every retail business will have unique priorities in monitoring fraud, reflected in the varying results. Compared with the wider survey average more retail businesses track fraud levels according to whether the order was placed on the website (73% vs 68% average) or on the mobile app (58% vs 52% average).

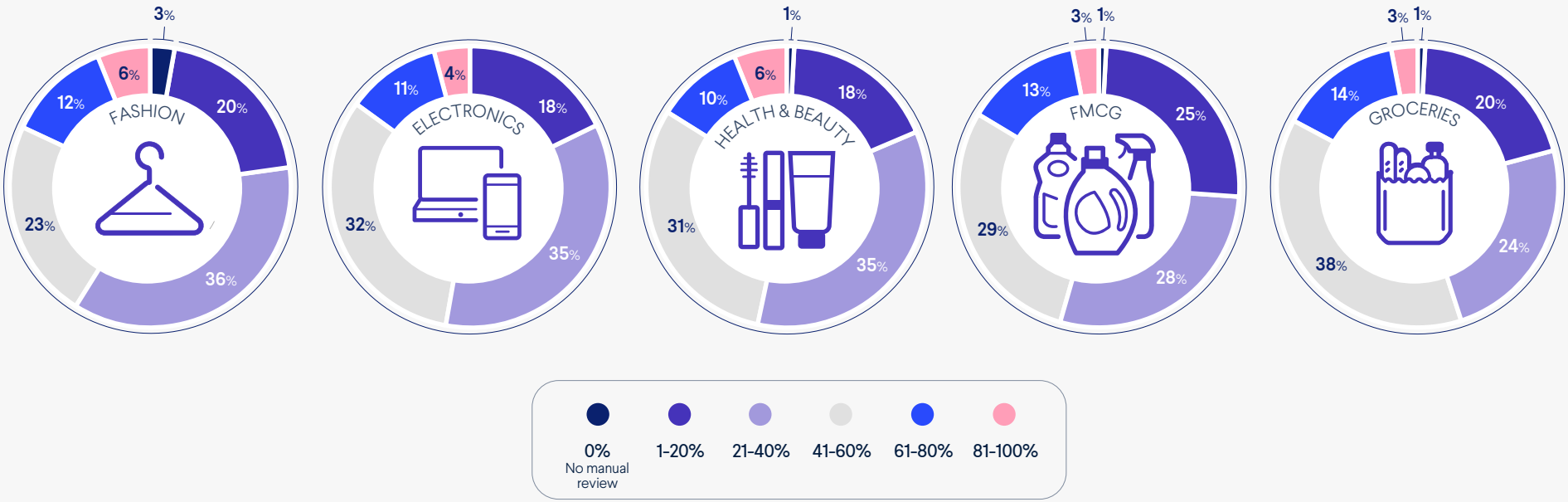
More retailers monitor customer acquisition route than other industries

More retailers monitor customer acquisition route than the survey average (46% vs 40%), perhaps because of greater use of social media marketing. Many fashion retailers use **socials like Instagram and twitter** to attract customers and offer exclusive promotions - for example ASOS has over 10 million followers on Instagram, 6.7 million on Facebook and another million on Twitter. Over half (52%) of fashion merchants monitor customer acquisition, perhaps finding that social media attracts fraud/promo abuse as well as customers.

TRACKING FRAUD BY **SPECIFIC DATA**



TIME SPENT ON MANUAL REVIEW



Manual review is still an important part of fraud prevention despite advances in fraud tools. Human insight and deep understanding of the individual business are both critical. However, as the customer desire for speed increases with the growth of ecommerce, teams might not have enough time for manual review, or could fall into the trap of spending too much time reviewing transactions. Retail merchants have more varied approaches to manual review.

Fashion retailers have the most broad responses to time spent on manual review

Fashion retailers have the most polarized responses to manual review, with both the highest percentage spending no time on manual review, and the highest percentage spending the majority of time on manual review. This variation could indicate inefficient fraud prevention tactics, especially as fashion retailers have typically smaller fraud teams, who should have time to spend on other tasks.

Grocery retailers spend the most time on manual review

Over half of grocery merchants (55%) said that they spend over 41%+ of time on manual review, more than any other vertical. Many grocery retailers sell high-risk and restricted products like alcohol and tobacco that require identification and are fraud targets, requiring more manual review.

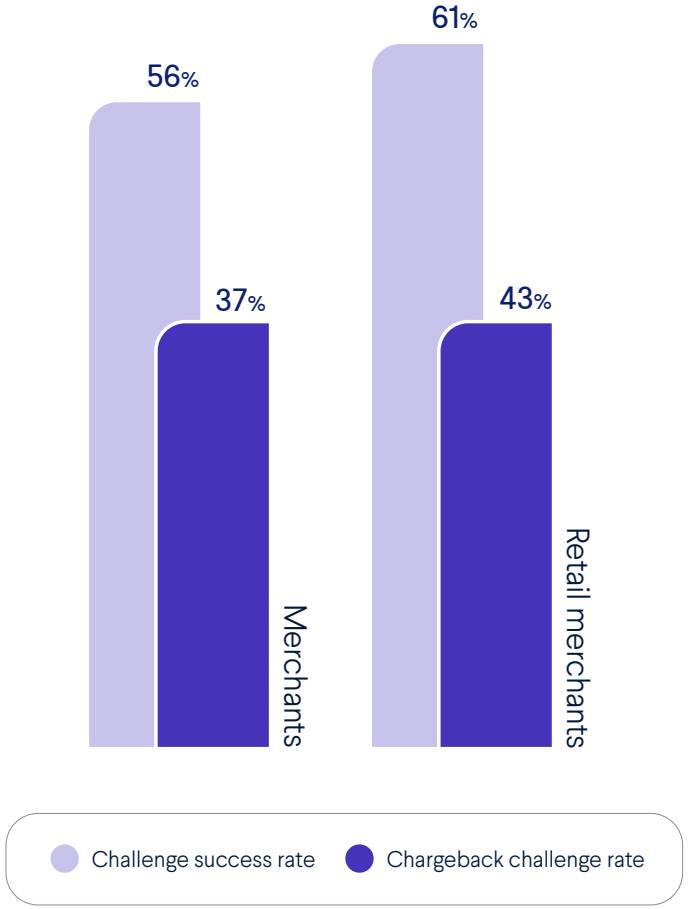
7.0 CHARGEBACK MANAGEMENT

Retailers challenge more chargebacks than other industries

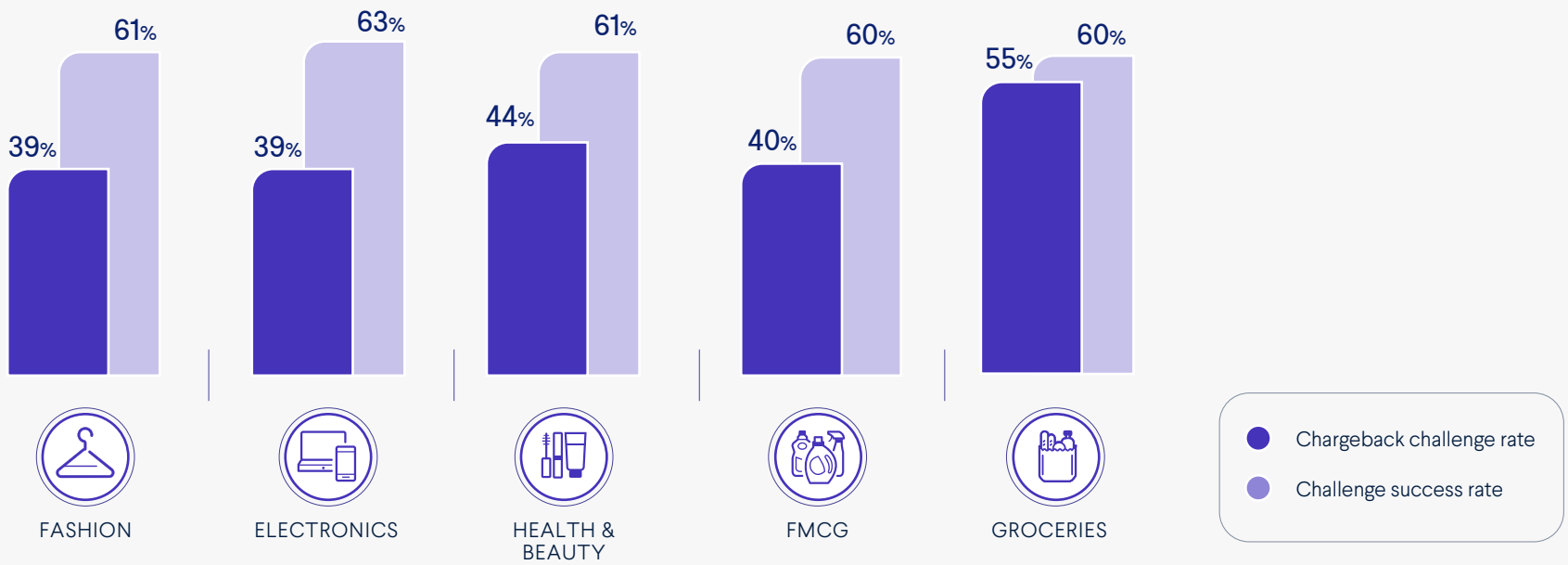
On average, companies challenge 37% of chargebacks and are successful in 56%. In retail, merchants challenge 43% of chargebacks and are successful in 61%. This means retailers receive more unjustified chargebacks than other industries. It is famously difficult for merchants to win chargeback disputes. According to card networks, **merchants tend to win just 21% of their disputes.** The retail average for winning disputes is far higher than this.

Not all chargebacks are the result of criminal fraud, and many cases are due to friendly fraud. Too many customers are filing unnecessary chargebacks, often unaware they are doing anything wrong.

RETAIL AVERAGES OF SUCCESS VS. CHALLENGE RATE



RETAIL AVERAGES OF SUCCESS VS. CHALLENGE RATE



Groceries challenge over half of chargebacks

Grocery merchants challenge 55% of chargebacks, with a 60% success rate. This suggests that over half of the chargebacks made against grocery businesses are unfair and worthy of challenging. Challenging over half of your chargebacks is a significant undertaking, taking time, patience and manpower.

Order fulfillment issues due to the pandemic could account for the high number of grocery merchant chargeback challenges. Grocery merchants working over-capacity are more likely to have delivery problems, unprocessed refunds, products not meeting specifications - the list goes on.

Fashion and electronics merchants challenge the fewest chargebacks

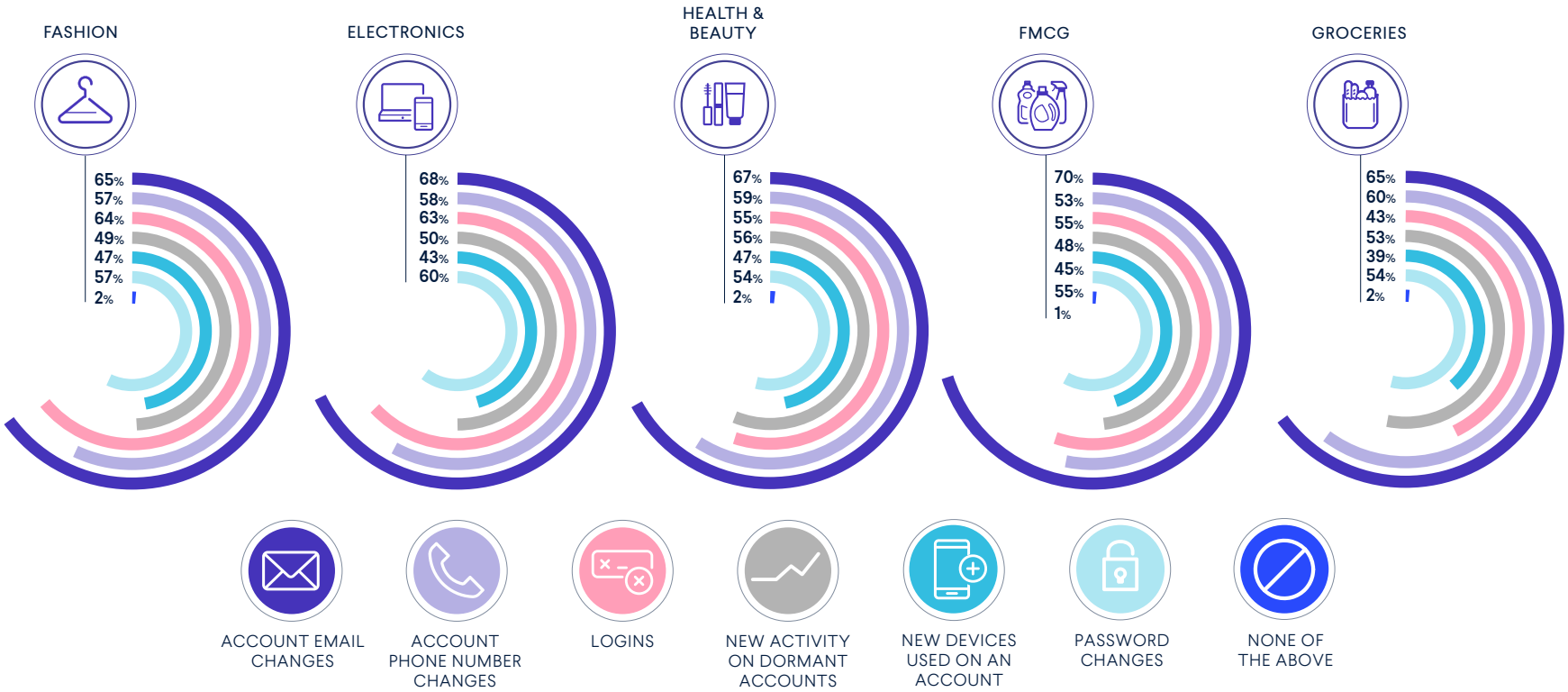
Fashion and electronics merchants both challenge only 39% of chargebacks, less than other retailers, perhaps accepting and paying more chargebacks, potentially at a bigger cost. Fashion was also most likely to have the smallest fraud team, and may not have the human resources to spend time challenging chargebacks. However, electronics are the most successful when challenging chargebacks, and typically have large teams.

8.0 ACCOUNT TAKEOVER

Retail merchants customer activity tracking

We asked merchants about the types of customer account activity they monitor, including key indicators of ATO attacks.

CUSTOMER ACTIVITY MONITORING BY RETAIL MERCHANTS

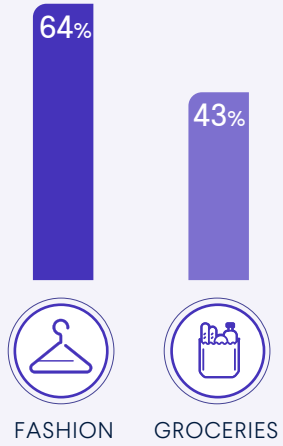


Retailers are leading the way with monitoring customer logins and new devices

Monitoring customer logins and new devices are a good first-defences against ATO, but relatively few merchants are tracking these in our wider multi-industry survey - with 55% monitoring customer logins, and only 40% new devices. Retail merchants are above average, with 56% monitoring logins and 47% new devices.

Fashion (64%) and electronics (63%) are leading with monitoring logins, bumping up the overall retail average. Monitoring logins can help fraud teams recognise credential stuffing - large scale automated login requests - a prolific ATO tactic. Monitoring and limiting login attempts can prevent ATO attacks getting out of control.

Fewer grocery merchants track logins (43%) and new devices added to an account (39%). We know that half of all grocery merchants reported a rise in ATO activity - this suggests that the true percentage who were targeted may be even higher.



Tracking customer logins

8.1 ACCOUNT TAKEOVER

Number of wide-ranging, high-impact ATO attacks

We asked retailers about how many wide-ranging, high-impact ATO attacks were targeted at their business in the past 12 months. These attacks must have impacted a significant proportion of the merchant customer base.

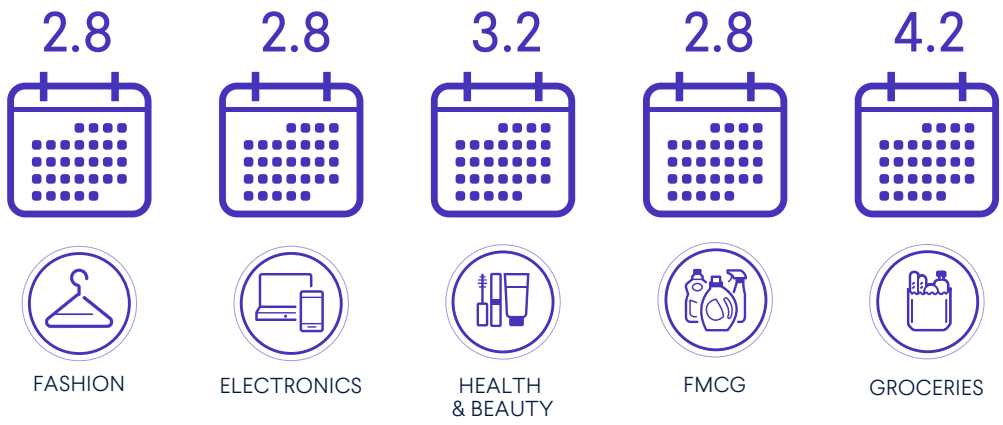
3

Retail merchants have an average of three ATO attacks per month

Retailers have seen fewer ATO attacks than other merchant categories, but they are still facing an average of three attacks per month.

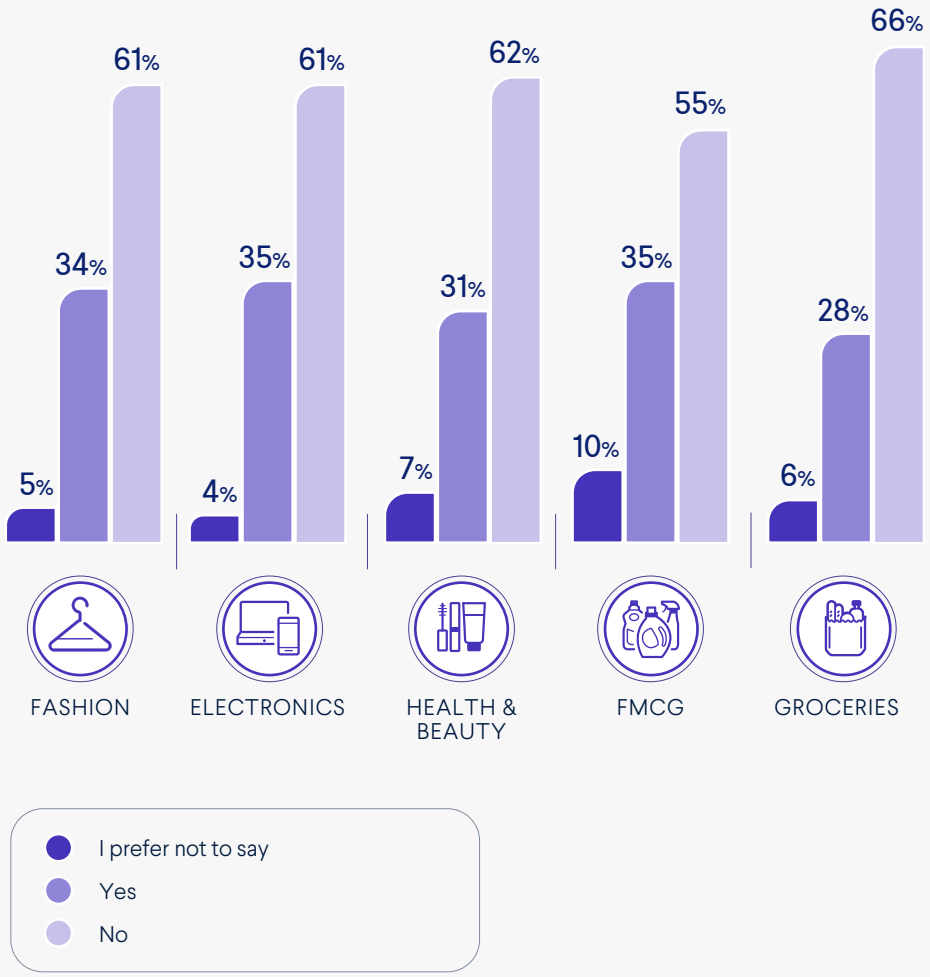
Grocery merchants are at the top end, experiencing an average of at least four attacks each month (53 attacks in 12 months). This is concerning as groceries merchants are also less likely to see ATO as one of their top three fraud risks than other retail categories, and are less likely to protect themselves by tracking logins and new devices added to accounts. Grocery merchants should perhaps stop underestimating the risks associated with ATO.

AVERAGE NUMBER OF **ATO ATTACKS PER MONTH**



Some retailers are not reporting ATO attacks

RETAIL RESPONSES ON WHETHER THEY
REPORT ATO ATTACKS TO AUTHORITIES



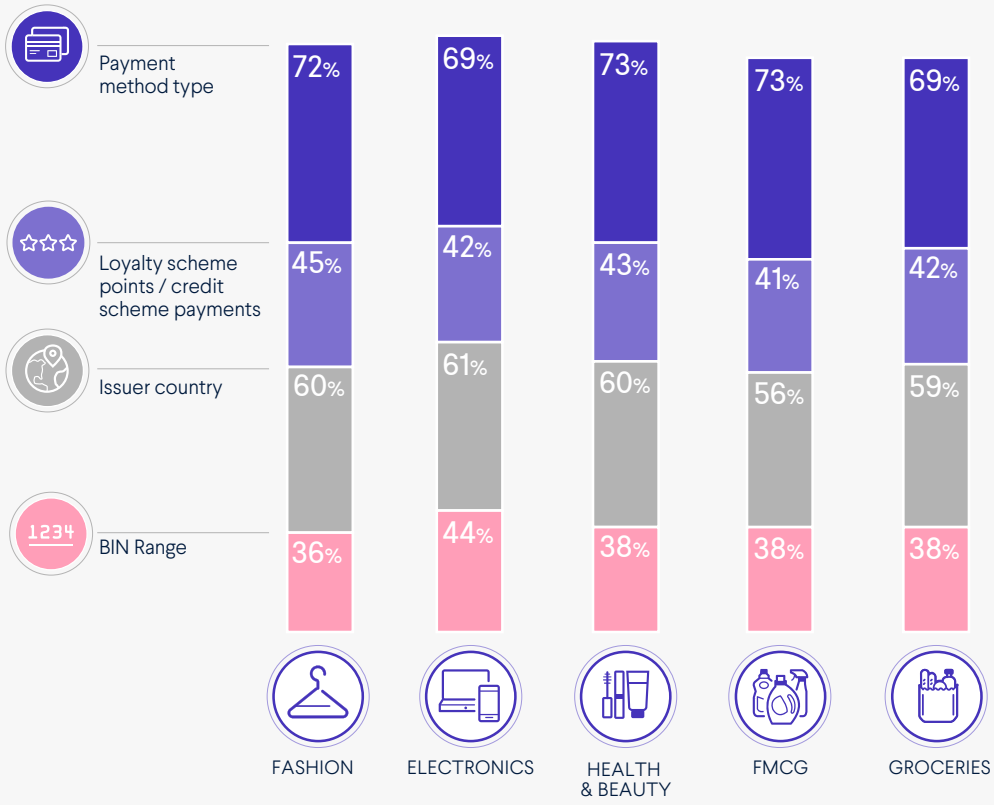
Not all retail merchants are reporting ATO attacks. For instance, grocery merchants had an average of 53 attacks in 2020, yet 28% did not report any at all. FMCG merchants are least likely to report ATO attacks, with only 55% saying they had done so in the past year, despite having an average of 2.8 ATO attacks per month.

This is a trend across all merchant industries, as only two-thirds (67%) of all merchants we surveyed reported ATO to the relevant authorities on data privacy. Merchant obligations to report ATO attacks under GDPR seem to be misunderstood. Even a small ATO attack is a data breach, and merchants must report them to the relevant authorities or they could be fined. We categorised an ATO attack as 'wide-ranging' and 'high-impact,' so every case should have been reported.

9.0 PAYMENTS

Tracking fraud trends by payment data

RETAIL MERCHANTS TRACKING FRAUD BY PAYMENT DATA



Slightly more retailers track fraud by issuer country (59%) than other industries (56% in our wider industry survey). Almost three-quarters of retailers track payment method type above the wider survey average of 67%. Tracking payment method type is important to understand the fraud your business is facing. Some payment types are more susceptible to fraud, but every business faces slightly different techniques and experiences different trends.

Electronics merchants are more likely to track fraud by BIN

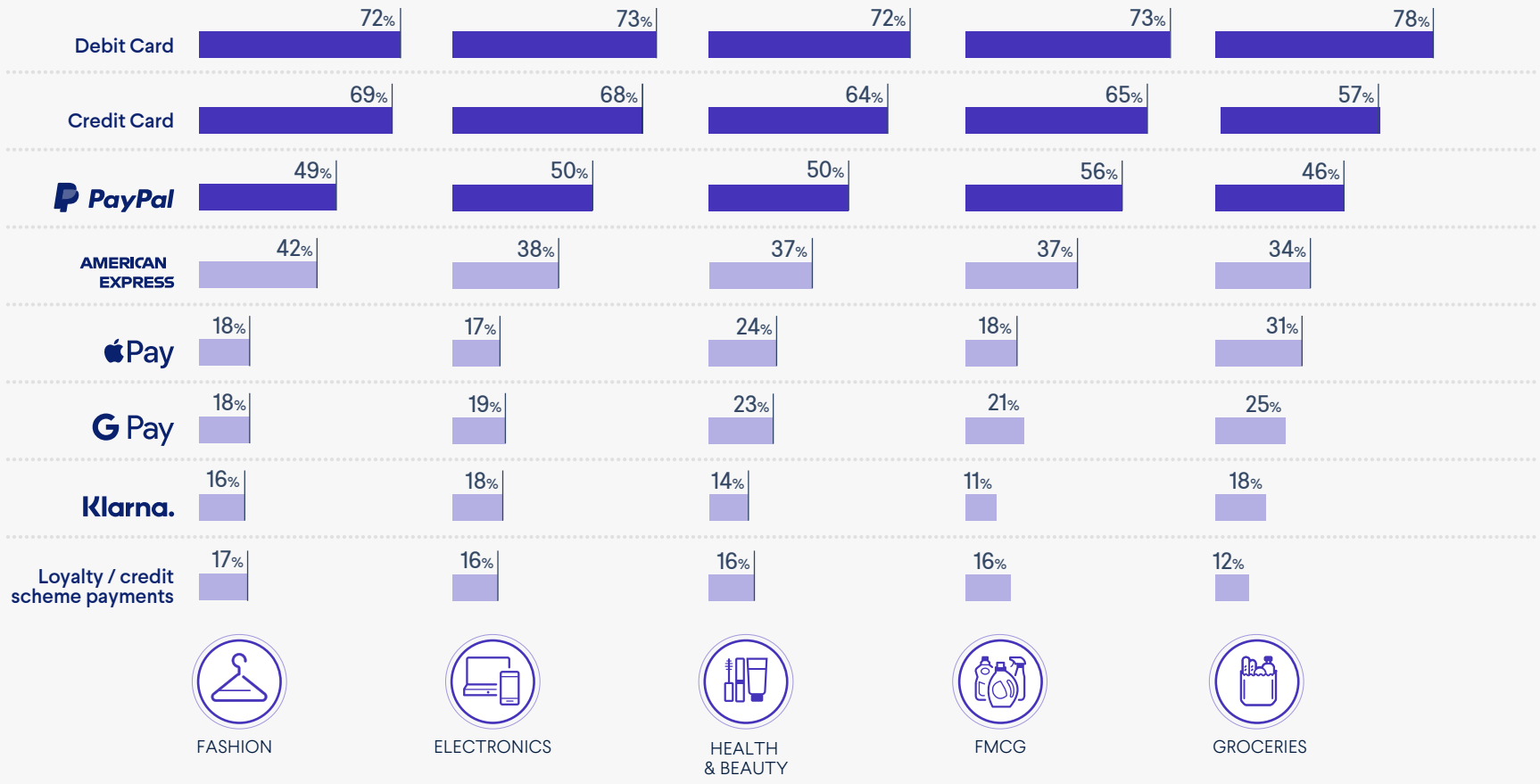
Retailers track BIN range more than other industries, as 39% of retail merchants track fraud by BIN compared to 31% in our wider industry survey average. Electronics pull up the retail average - 44% of electronics retailers track the BIN, over only 38% in every other vertical. Electronics merchants have larger fraud teams which may mean they have more resources and time to invest in managing fraud and payments.

Due to the high value of electronics goods, they could be more of a target for **BIN attacks**. BIN numbers can also help identify card issuer countries, and electronics retailers find location a valuable indicator of fraud (61% track issuer country).

Retailers see the most fraud on debit cards, credit cards and PayPal

We asked merchants about the top three payment methods where they see the most fraud.

TOP THREE PAYMENT METHODS FOR FRAUD



GooglePay and ApplePay as payment methods for fraud

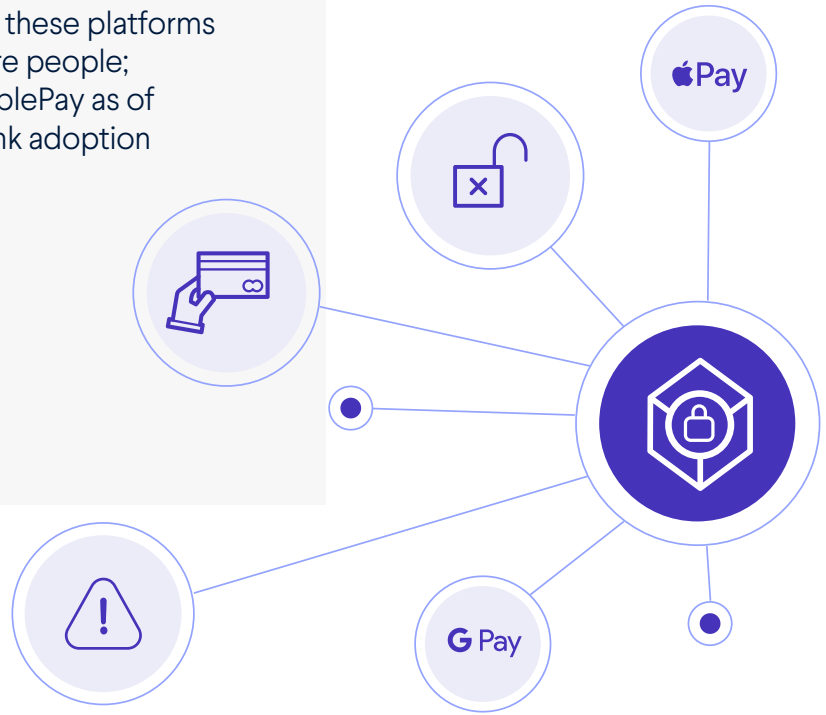
Grocery retailers have seen more fraud on GooglePay and ApplePay than other retail merchants, with 31% ranking ApplePay in their top three, and 25% giving GooglePay a top spot. This is above the 22% (ApplePay) and 21% (GooglePay) retail averages.

Customers are less likely to use cash due to pandemic hygiene concerns, perhaps using smartphone payments as a convenient substitute. ApplePay and GooglePay have no contactless upper limit, so if fraudsters put fake or stolen credit cards on their smartphones, they can gain a lot - you could buy a large grocery shop in-store using these payment methods without entering a pin. Supermarkets have been the only possible target of card-present fraud, perhaps accounting for these smartphone fraud concerns.

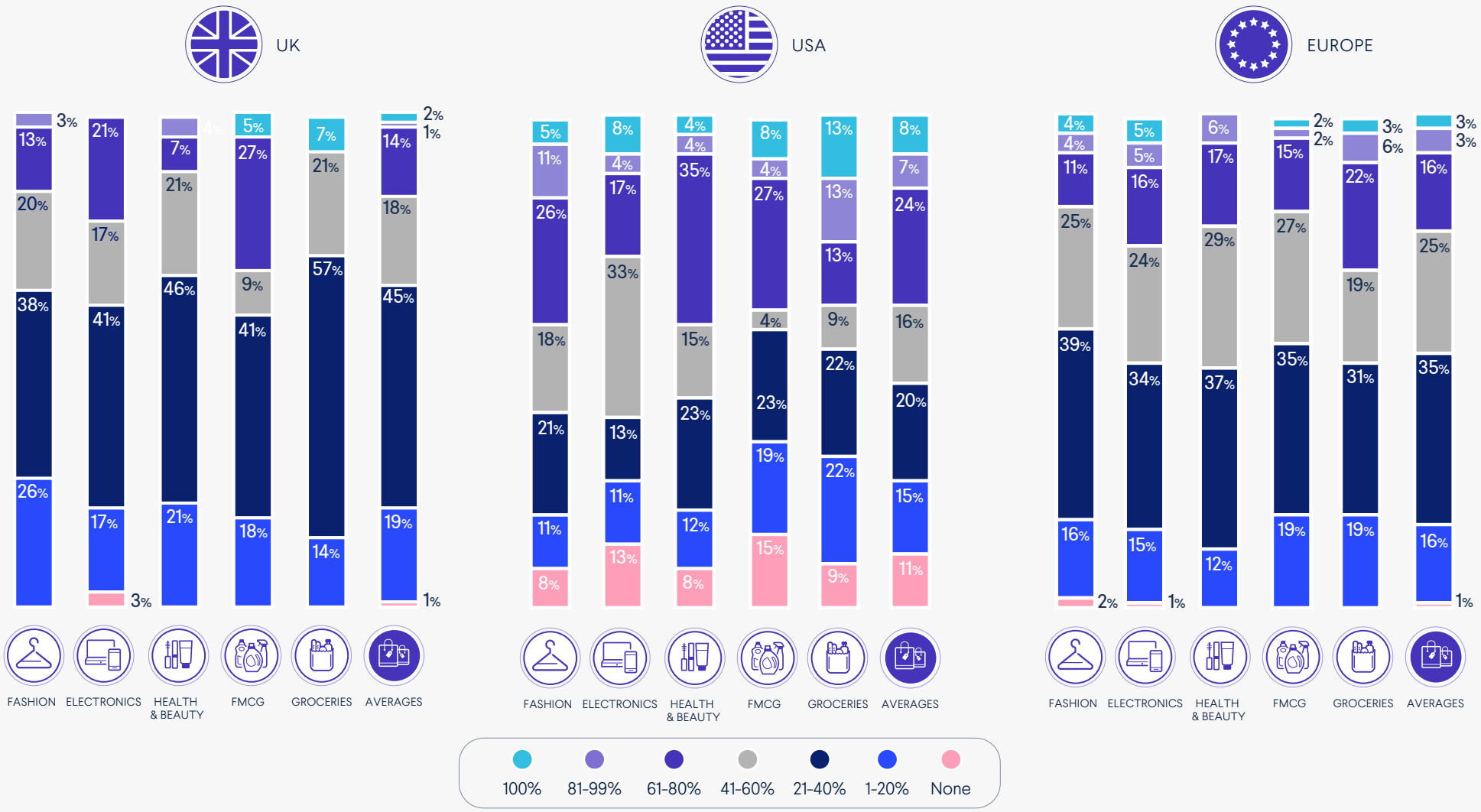
Almost a quarter of retailers put GooglePay and ApplePay in their top three payment methods in which they see the most fraud. These smart mobile payment methods claim to be safer, with biometric authentication and encrypted customer details, but users can still add fraudulent card details to their virtual wallets. Fraud will continue to develop on these platforms as they are adopted by more people; **507 million iPhones** use ApplePay as of September 2020, a YoY bank adoption growth of 20%.

25%

One-quarter of retailers put GooglePay and ApplePay in their three most fraudy payment methods.



TRANSACTIONS GOING TO 3D SECURE **BY LOCATION**



UK retailers are currently sending less traffic to 3DS than US or European retailers. A large chunk of UK retail merchants (45%) are only utilising 3DS 21% to 40% of the time.

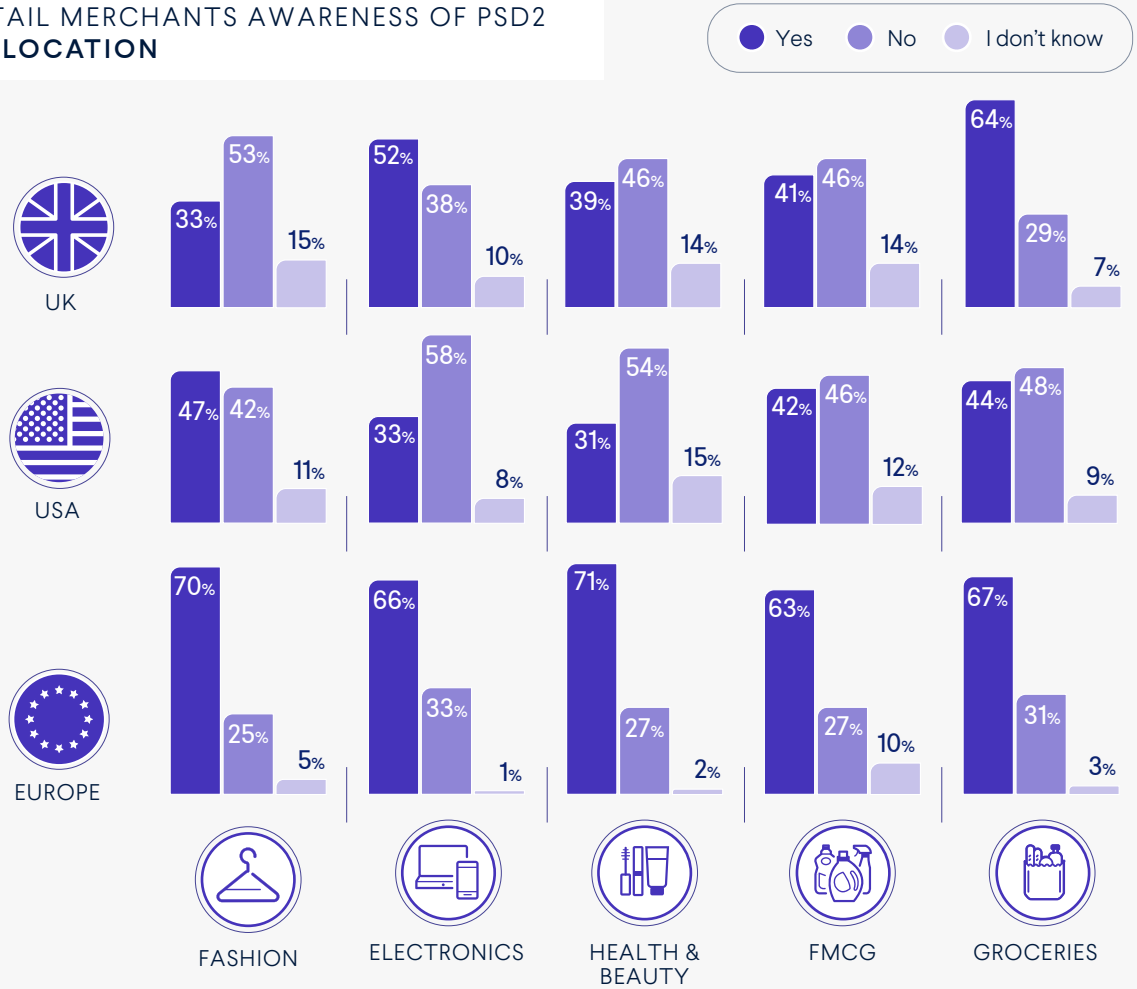
Comparatively, US retailers are more polarized, as around a quarter (24%) send traffic to 3DS 61% to 80% of the time, and a quarter (26%) also send to 3DS from 0-20% of the time.

The results for Europe were more balanced, with 60% falling in categories from 21 to 60%. The fact that the majority of European merchants are already using 3DS frequently is promising in the context of PSD2.

10.0
EUROPE'S PSD2 REGULATION

Retail merchants awareness of PSD2

RETAIL MERCHANTS AWARENESS OF PSD2
BY LOCATION



We asked merchants whether they think PSD2 will impact their business to understand the level of understanding and readiness.

On average, 42% of UK retailer merchants wrongly think PSD2 will not impact them, and 12% don't know. In January 2021 the UK officially left the EU, potentially leading UK-based retailers to think they are now exempt. PSD2 does apply in the UK, retailers need to educate themselves on the authentication changes that will be enforced in the UK from September 2021.

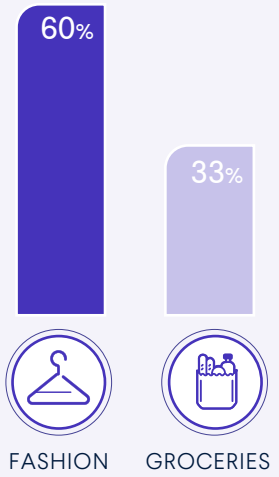
Europe-based retailers seem to have a greater understanding of PSD2, as around two-thirds recignose that PSD2 will impact them. Whilst this is an improvement, over a quarter are still unaware that their business will be affected by a major European regulation.

When it comes to US-based retailers, 39% think it will impact them, 50% think it won't and 11% don't know. US merchants that voted 'yes' may trade within the UK or European countries, and will be directly impacted, but even those who voted 'no' may face indirect economic backlash down the line as **fraudsters target non-European payments with looser controls.**

Gap between grocery and fashion retailers

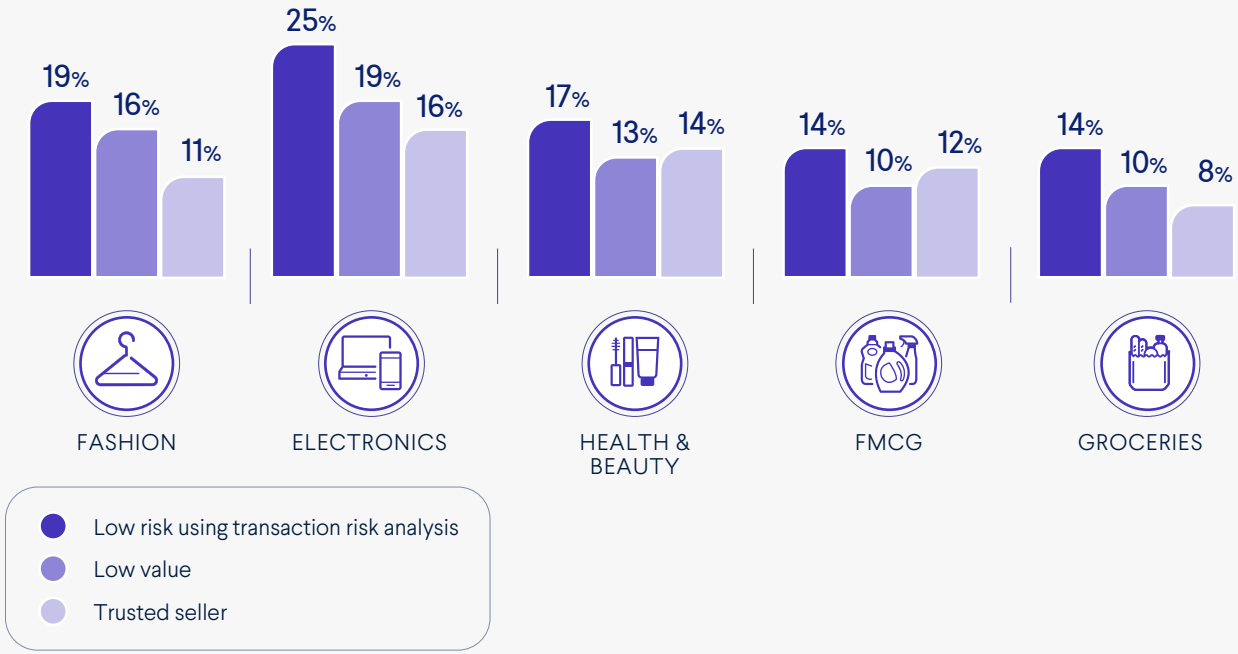
Over 60% of UK grocers understand the impact of PSD2. UK fashion retailers are in the dark by comparison, as only a third (33%) think PSD2 will impact them, with over half (53%) thinking it won't.

European fashion retailers are better informed, as 70% understand that PSD2 will impact them. These massive divides in PSD2 understanding between retail industry verticals and between the UK versus Europe are worrying. Perhaps payment service providers are not doing enough to educate business owners affected.



Fewer UK retailers understand the impact of PSD2

MERCHANTS PLANNED USE OF **EXEMPTIONS**



Merchants planned use of PSD2 exemptions to SCA

Very few retail merchants are planning to use exemptions to SCA under PSD2. This could be because merchants had not yet formed a strategy for PSD2 at the time of the survey (August 2020). PSD2 is a complex regulation, and as many retail merchants were not aware of the impact PSD2 may have on their business, it's likely that the exemptions are not fully understood by all. Learn more about the impact of PSD2 and how to develop your strategy to prepare for exemptions in this webinar featuring **Marco Conte, Co-Founder of Payment Universe consultancy.**

11.0 SUMMARY

Retail merchant responses in this survey give us a valuable, in-depth understanding of the environment facing today's retail fraud teams, and forecasts for what's to come. The high-level insights also highlight where further investigations and discussions can enable merchants to boost their fraud detection ability, and gain deeper knowledge on their customers and the threats they face.

1

COVID-19 IMPACT ON RETAIL FRAUD TEAMS IS SEEN AS LARGELY POSITIVE

Many retailers are benefiting from ecommerce booming - particularly groceries merchants. This pandemic positivity correlates with improvement in business perception of the fraud team.

2

RETAIL FRAUD TEAMS WILL GET BIGGER AND BETTER IN 2021

Retail fraud teams are likely to be larger than other industries, especially in electronics. All retail fraud teams expect growth in 2021, tied to wider business perception of the fraud team improving.

3

FRAUD BUDGETS WILL INCREASE AS FRAUD SOLUTIONS NEED TO BE MORE AGILE

Merchants are investing in fraud teams to arm themselves against growing risks. But, as machine learning, graph networks and device ID tools are less widely used, there are some notable gaps in the retailer's fraud toolkit.

4 REFUND ABUSE SURGES BUT ONLINE PAYMENT FRAUD IS STILL THE BIGGEST RISK

Whilst retailers consider online payment fraud to be the biggest risk, the rising risks of refund abuse shouldn't be overlooked.

5 RETAILERS ARE RECEIVING AND CHALLENGING LARGE AMOUNTS OF CHARGEBACKS

Retailers receive a significant amount of unjustified chargebacks, but they are also challenging more than all other industries.

6 RETAILERS FACE SIGNIFICANT ATO ATTACKS, BUT MANY GO UNREPORTED

All retailers have frequent ATO attacks, with grocery merchants experiencing 4+ attacks per month, but not all retailers report them. Fortunately, more retail merchants enforce 2FA than other industries.

7 RETAILERS SEE THE MOST FRAUD ON DEBIT CARDS, CREDIT CARDS AND PAYPAL

Most retailers track fraud on payment methods, with a high number of merchants suffering significant fraud on GooglePay and ApplePay. UK retailers currently send less traffic to 3DS than merchants in the US or Europe.

8 SIGNIFICANT NUMBERS OF UK RETAILERS ARE NOT AWARE OF PSD2'S IMPACTS

Almost half of UK retailers wrongly think PSD2 will not impact them - merchants in Europe and the US are more aware of the effects. Very few retail merchants plan to use exemptions to SCA, indicating lack of understanding.

Thank you for reading this survey report

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

GET IN TOUCH

Learn more about Ravelin's fraud and payments services at

ravelin.com