Ravelin

FRAUD IN A SHORT-ATTENTION ECONOMY

WHY IT'S TIME FOR A FRESH APPROACH

CFO PERSPECTIVES FROM ONLINE BUSINESSES GLOBALLY

FOREWORD BY MARTIN SWEENEY, RAVELIN CEO

Brands are fighting on two fronts today, to retain discerning consumers, while protecting and growing their business in a challenging economic climate.

Nowhere is this more keenly felt than in e-commerce. "Quick commerce" services for food deliveries and taxis are setting the new standard for customer experiences, and people today expect the same experience from every brand they buy from online. It is no wonder that almost 90% of UK shoppers are saying they will abandon a purchase because of "friction" - additional stages on the customer journey, which include checks for fraud.

Yet no online business can afford to turn a blind eye to fraud. Losses due to card not present fraud, the most common type of fraud in e-commerce, reached nearly £200m in the first six months of 2022 alone (UK Finance).

Our survey of CFOs at online merchants around the world finds that fraud continues to be a significant contributor to profit erosion.

Payment card fraud by criminals remains high, but fraud by merchants' own customers runs closely behind. Around half of finance leaders surveyed agree fraud by customers, including "friendly fraud", promotions, and refunds abuse, has increased compared with a year ago.

We find that the stock response to growing fraud is to throw more money and resources at it: bigger fraud teams, more processes. Yet this is unsustainable: fraud will continue to mutate, customers will become more demanding and fickle, losses will continue to grow.

To stay relevant to time-poor customers, minimise losses, and emerge stronger from the current economic slowdown, brands need to think differently about managing fraud. They need to automate more, and rely less on manual investigations. Fixed rules need to give way to machine learning.

This report focuses on the perspectives of Chief Financial Officers, who generally have overall responsibility for fraud. We asked them about their fraud experience over the last 12 months and what they expect in the coming year. How are they handling this increasingly complex landscape, and what's the impact on their business? We've laid out our key findings here.

Methodology

Ravelin commissioned research provider Qualtrics to carry out an online survey of 1,900 e-commerce leaders from merchants across 10 countries, including CFOs, CTOs, Chief Risk Officers, and fraud and payments managers. Survey participants work for online merchant businesses with more than $50 million in annual revenue.

CONTEXT

Businesses around the world are facing unprecedented challenges. The last few years have seen them reacting to a global pandemic and significant political, economic and societal change.

In the UK, the cost of living crisis is contributing to reduced consumer spending and a rise in fraud. More and more opportunistic fraudsters take their chances, while professionals are becoming more sophisticated in their tactics. Respondents tell us that they have seen fraud increasing across the board (see chart 1).

The Covid-19 pandemic has had an impact too. 35% of CFOs say that Covid-19 increased fraud in their business, and they see new types of fraud. The pandemic has raised awareness of fraud across the business (according to 53.4% of CFOs). This is leading to bigger budgets (48.1%) and a greater focus on stopping fraud.

35%

of CFOs are seeing increased, more sophisticated fraud

CHART 1: How much of the following types of fraud are you experiencing, compared with a year ago?

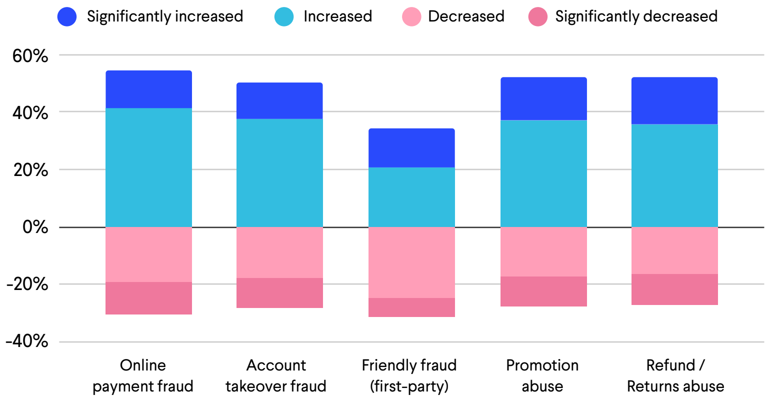
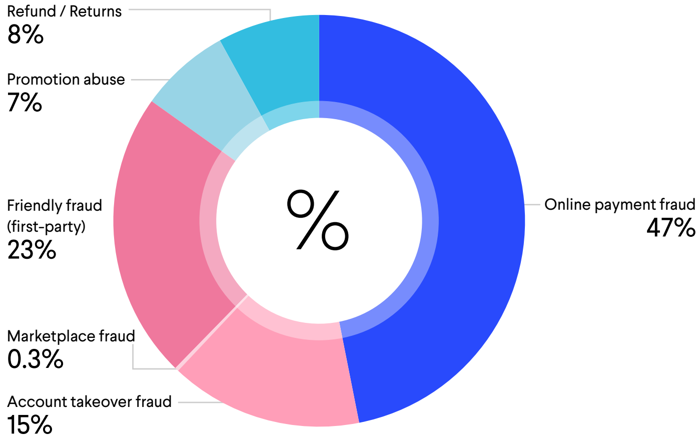
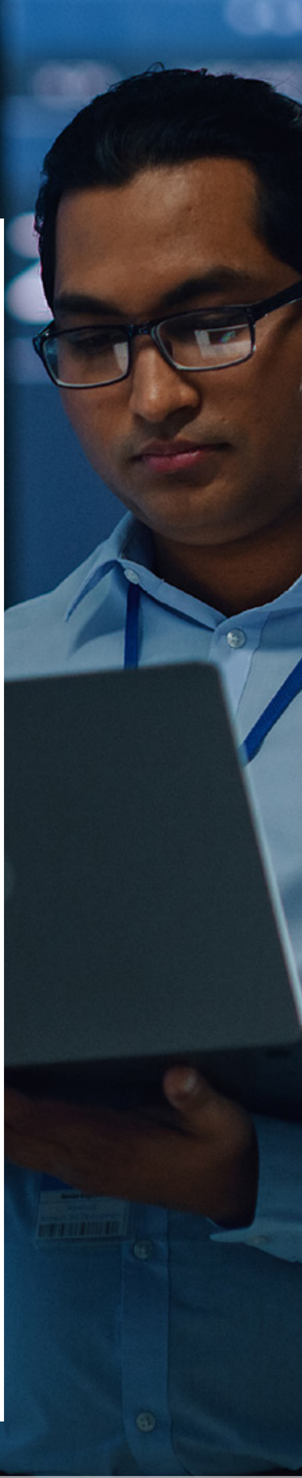


CHART 2: Respondents rating each risk factor as 1 = highest risk to their business





THE RISE OF THE “CRIMINAL CUSTOMER”

Our survey finds that merchants’ own customers are almost as likely to commit fraud against them as organised criminals, a trend which is likely to have been accentuated by the cost of living crisis.

A significant proportion of the fraud reported by respondents is “first party” fraud - i.e. from their own customers. Over a third of finance leaders describe first party frauds including “friendly fraud”, returns, and promotions abuse, as the number one risk factor facing their business.

The trend seems particularly pronounced among younger age groups. A study by fraud agency CIFAS found one in 13 people admitted to involvement in some form of first-party fraud - rising to one in seven among digitally-savvy 16-34 year olds.

1 in 3

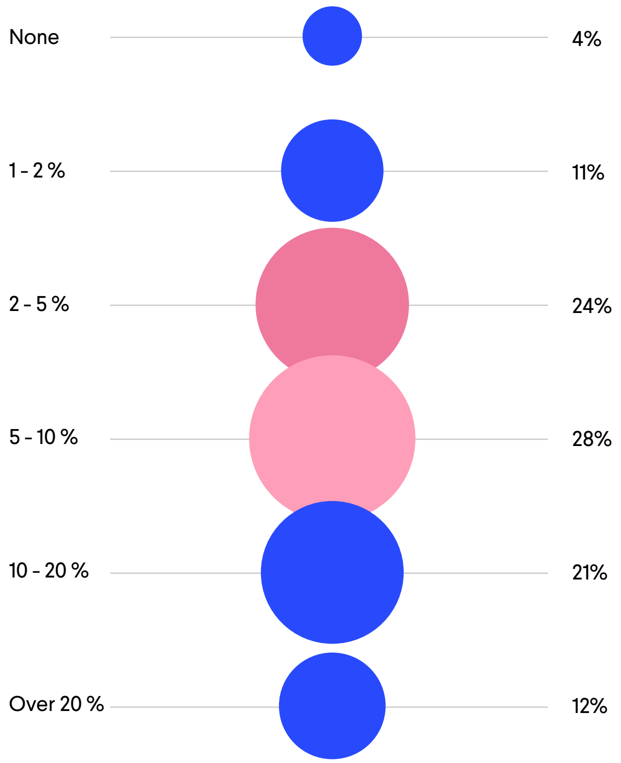
finance leaders describe “friendly fraud”, returns, and promotions abuse, as #1 risk factors for their business

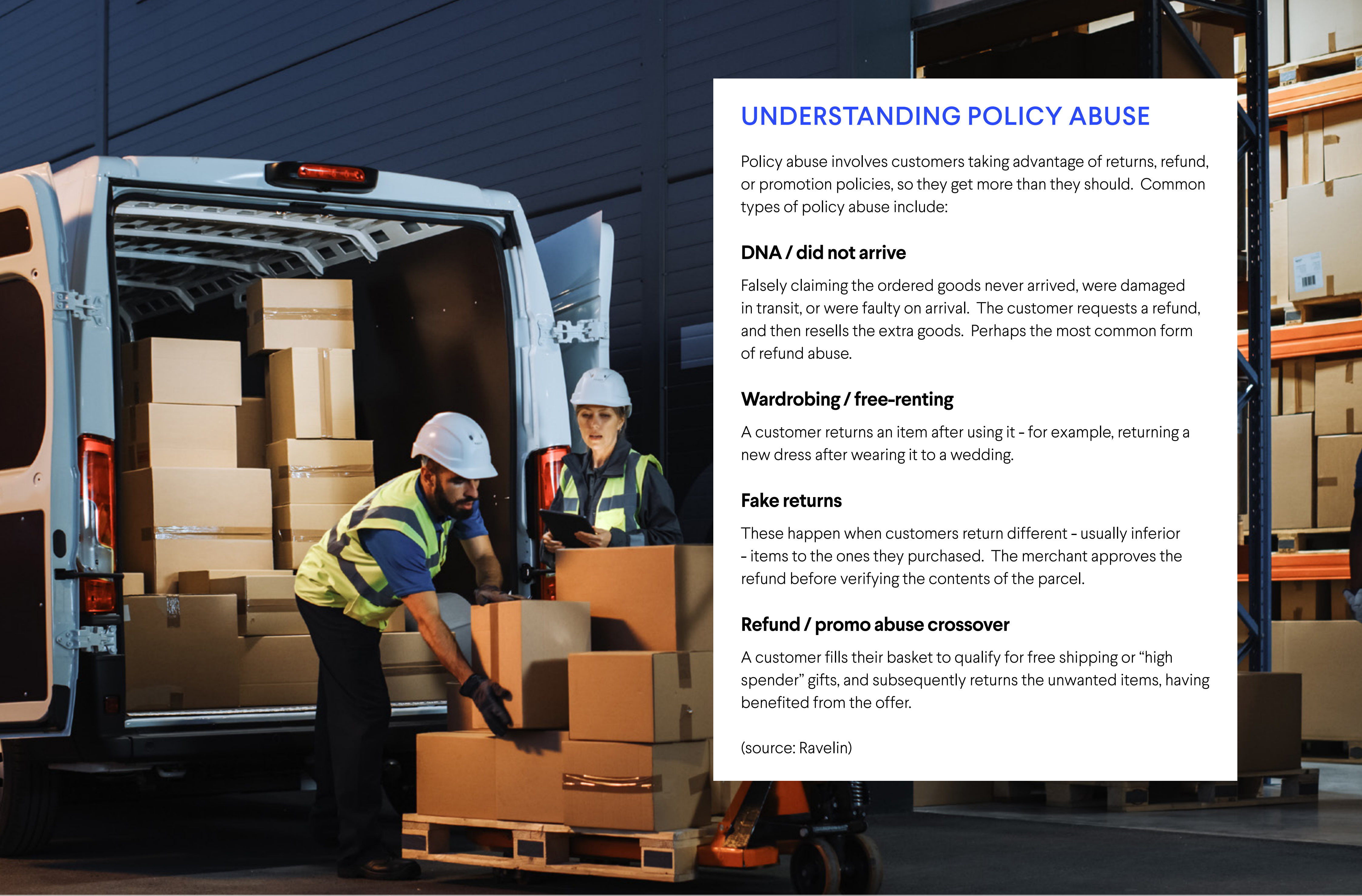
›50%

of respondents report increases in promotions and refunds abuse during 2022

Policy abuse, deliberately taking advantage of returns and exchanges or discounts, is a growing problem that can greatly impact the bottom line (see box overleaf). Almost a third of the finance leaders in our survey believed 10 percent or more of their returns to be fraudulent (chart 3).

CHART 3: In the last 12 months what percentage of all returns or refunds do you estimate to be a result of abuse of policy?





UNDERSTANDING POLICY ABUSE

Policy abuse involves customers taking advantage of returns, refund, or promotion policies, so they get more than they should. Common types of policy abuse include:

DNA / did not arrive

Falsely claiming the ordered goods never arrived, were damaged in transit, or were faulty on arrival. The customer requests a refund, and then resells the extra goods. Perhaps the most common form of refund abuse.

Wardrobing / free-renting

A customer returns an item after using it - for example, returning a new dress after wearing it to a wedding.

Fake returns

These happen when customers return different - usually inferior - items to the ones they purchased. The merchant approves the refund before verifying the contents of the parcel.

Refund / promo abuse crossover

A customer fills their basket to qualify for free shipping or "high spender" gifts, and subsequently returns the unwanted items, having benefited from the offer.

(source: Ravelin)

THE ENTREPRENEURIAL FRAUDSTER

Criminal fraud enterprises are growing in sophistication. Capitalising on a generally higher propensity for fraud, CFOs have seen an increase in more sophisticated schemes like “fraud-as-a-service”. They also say account take-over and reseller activity - most likely the work of organised criminals - are all on the up, while newer types of fraud, like bot activity, are emerging.

58%

of CFOs agree that reseller and bot activity are the newest types of fraud impacting their businesses

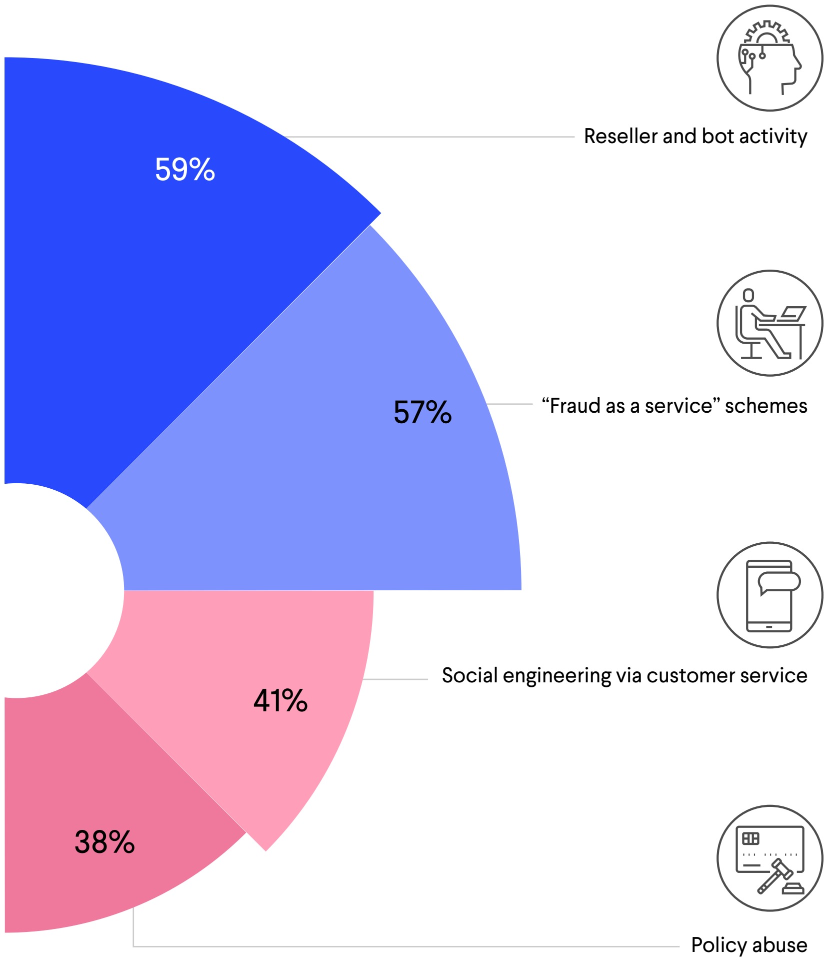
57%

are seeing growing fraud-as-a-service schemes

CFOs rank account take-over as one of the biggest risk factors to their business

22.6% rank it the top risk factor,
28.8% rank it second

CHART 4: What are some of the new types of fraud trends that your business is seeing? (multiple answers accepted)



BREAKING AND ENTERING ONLINE

Fraudsters who gain access to a customer's account - called account takeover - generally place an order 71% of the time and get away with it 50% of the time. The cost to businesses goes beyond the financial: victims generally blame the merchant for lax security - often publicly. This makes the fallout far wider than the incidents themselves.

Our survey found losses from account takeover alone run into millions of dollars each year, with four in ten respondents reporting annual losses in excess of $5m. The costs are primarily loss of revenue and personal data theft, and associated fines.

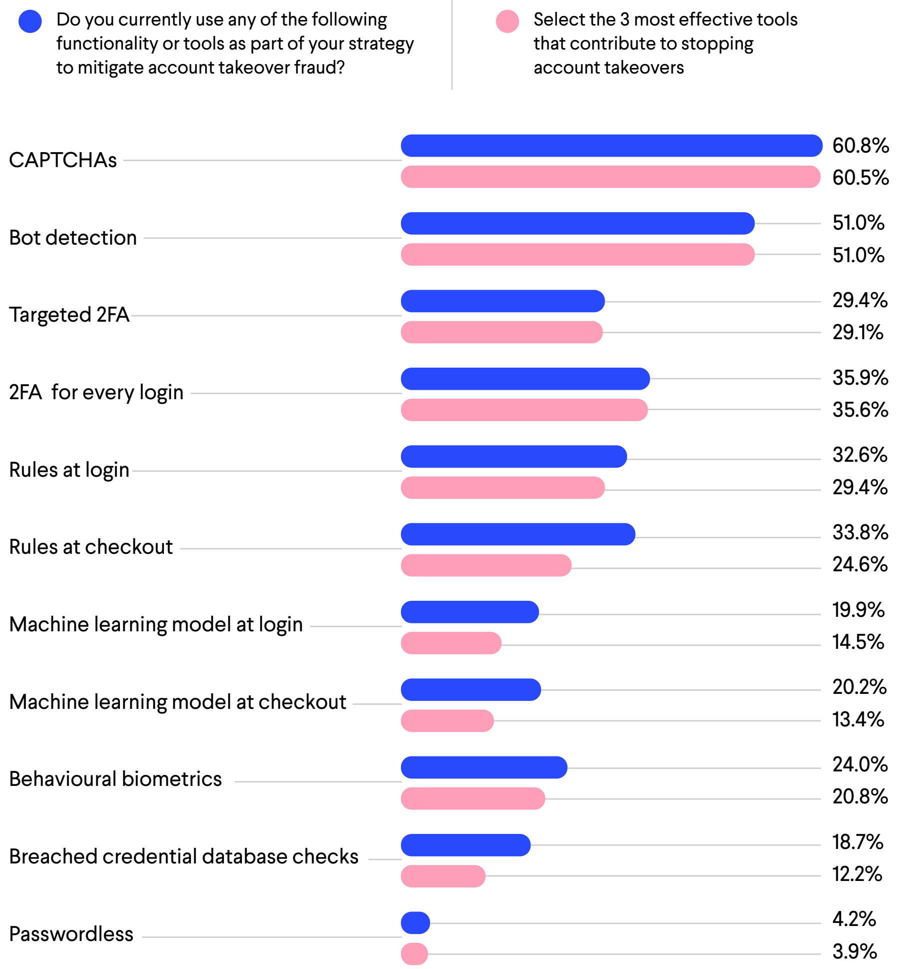
43%

of finance leaders report losing over $5m each year as a result of account takeover

The reputational costs of account takeovers are substantial. Sixty percent of respondents say they have been featured in the press or social media because of account takeovers at least once last year. Customers often blame the merchant for poor security, resulting in a loss of customer trust, low retention, and a decrease in the customer's lifetime value.

Given the unique risk profile of account takeover, it's no surprise that almost every CFO - 98.6% - has invested in tools to detect or prevent it. As chart 5 shows, respondents voice a clear preference for mechanisms like CAPTCHA and bot detection, which can add extra steps to the customer journey. However, use of rules and machine learning to automate the detection of account takeover is less widespread.

CHART 5:



PAYMENTS: FRAUD NOW, PAY LATER?

Almost 40% of shoppers across Australia, the UK, and the United States say they are initiating more disputes today than before the Covid-19 pandemic. CFOs are feeling the consequences - 47% of them rank online payment fraud as the biggest threat to their business.

Our survey finds debit (highlighted by 63% of respondents) and credit cards (68%) remain the most commonplace vectors for card fraud. These are, however, the easiest for merchants to successfully challenge in a fraud dispute.

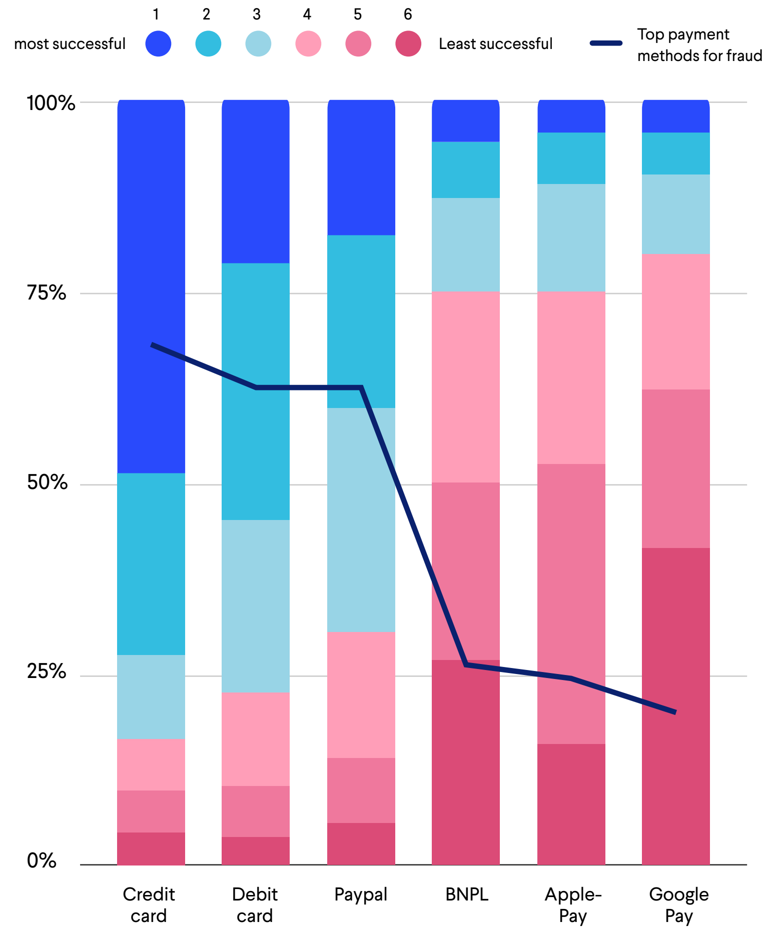
On the other hand, new forms of payment like Apple Pay, Google Pay and Buy Now Pay Later (BNPL) schemes like Klarna are more likely to represent a headache for online merchants regarding dispute resolution (chart 6). Though CFOs say they currently experience less fraud via these methods, they consider them far harder to successfully challenge.

60%

of CFOs say their fraud teams manage disputes alongside other responsibilities

When it comes to fraud investigations and disputes, a majority of CFOs (60%) say their fraud teams handle these alongside other tasks. This is additional, time-sapping work that takes fraud teams away from their core strategic roles and can be costly.

CHART 6: Prevalence of fraud (and effectiveness at challenging disputes) across payment methods



AUTHENTICATION: PROTECTION FROM FRAUD VS. CUSTOMER CONVENIENCE

Payment card authentication schemes, such as 3D Secure (3DS), offer an additional layer of security to both cardholders and merchants. They transfer liability for any fraud from the merchant to the issuing bank (though merchants must comply with any information requests from banks relating to fraud investigations).

It is no surprise, therefore, that almost every CFO in our survey considers 3DS either important (28.2%) or very important (70.6%) to their fraud prevention strategy. Meanwhile, 50% see PSD2 regulations, which facilitate customer data sharing between banks and merchants, as having a slightly positive impact on their business, and 27% say it's extremely positive.

Mainly driven by regulation and card scheme requirements, brands have been sending more customers through additional authentication over the last 12 months.

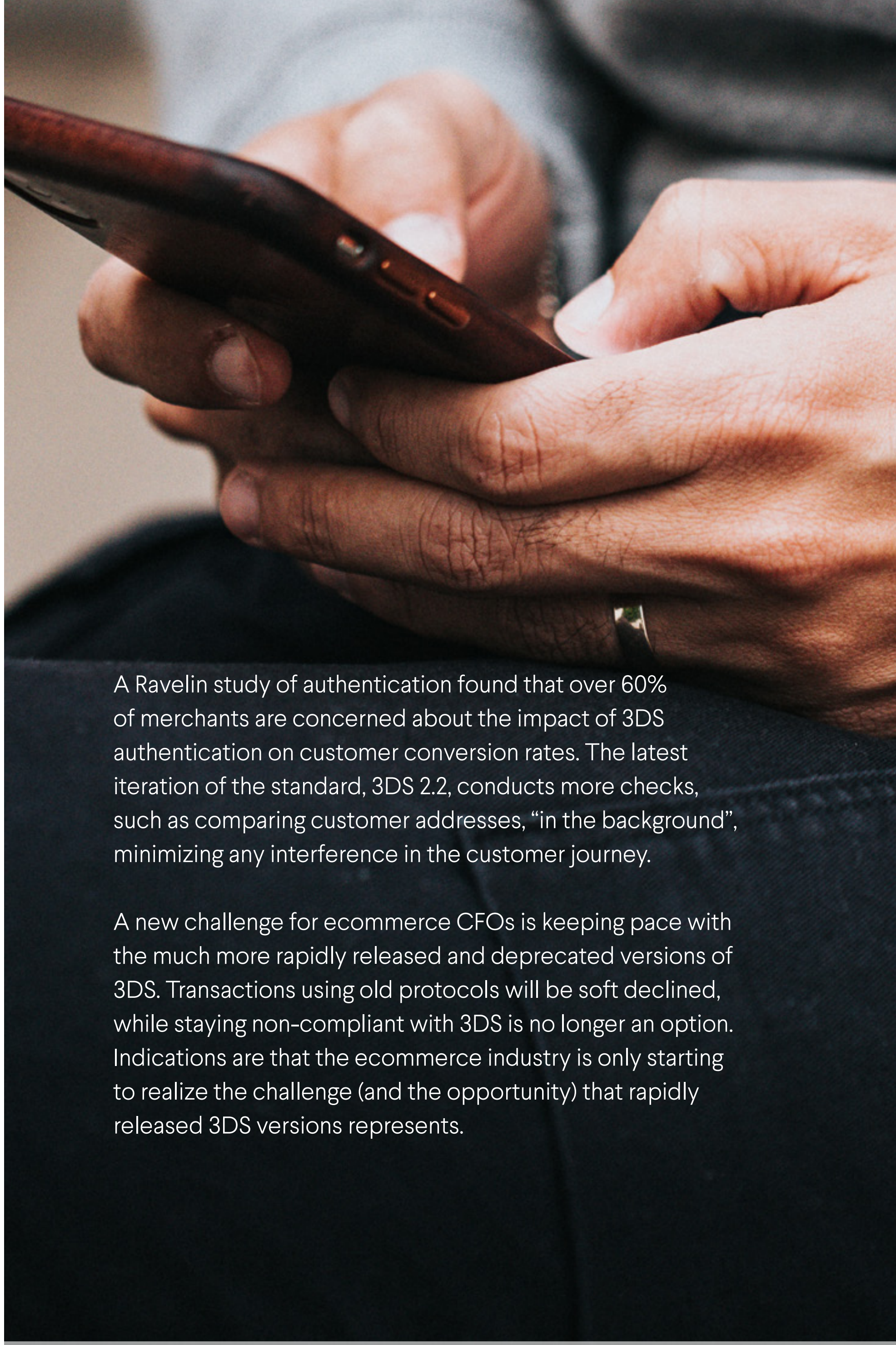
47.5%

of finance leaders say they've increased the amount of traffic they're sending for 3DS authentication

20.5%

have significantly increased authentication

The survey found that 51.3% of CFOs expect to send more traffic to authentication over the coming 12 months, with 24% expecting it to significantly increase.



A Ravelin study of authentication found that over 60% of merchants are concerned about the impact of 3DS authentication on customer conversion rates. The latest iteration of the standard, 3DS 2.2, conducts more checks, such as comparing customer addresses, "in the background", minimizing any interference in the customer journey.

A new challenge for ecommerce CFOs is keeping pace with the much more rapidly released and deprecated versions of 3DS. Transactions using old protocols will be soft declined, while staying non-compliant with 3DS is no longer an option. Indications are that the ecommerce industry is only starting to realize the challenge (and the opportunity) that rapidly released 3DS versions represents.

HOW FINANCE LEADERS ARE MANAGING FRAUD TODAY

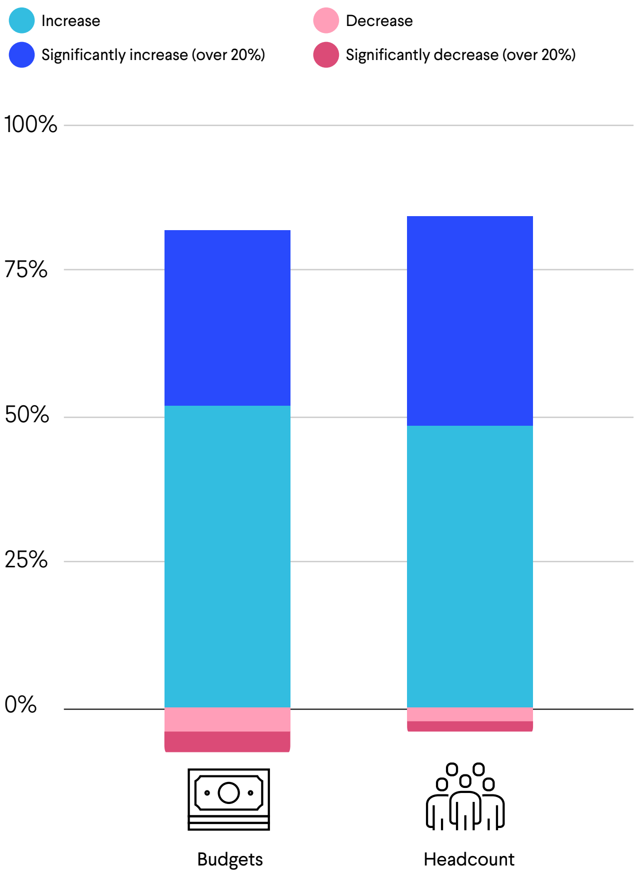
In spite of the evolving fraud landscape and the significant losses, finance leaders view fraud management as a largely manual and people-powered process. In other words, CFOs expect fraud management to become more expensive and resource-hungry.

Our survey finds most fraud teams are over ten people in size, and many are more than double that. Over 80% of respondents expect these teams to grow in size over the next twelve months, while only 4% expect their fraud teams to get smaller.

Fraud management budgets are increasing in tandem. Almost one in three finance leaders (31%) expect fraud budgets to increase by 20% or more this year. By comparison, only eight percent of respondents expect any kind of decline (chart 7)

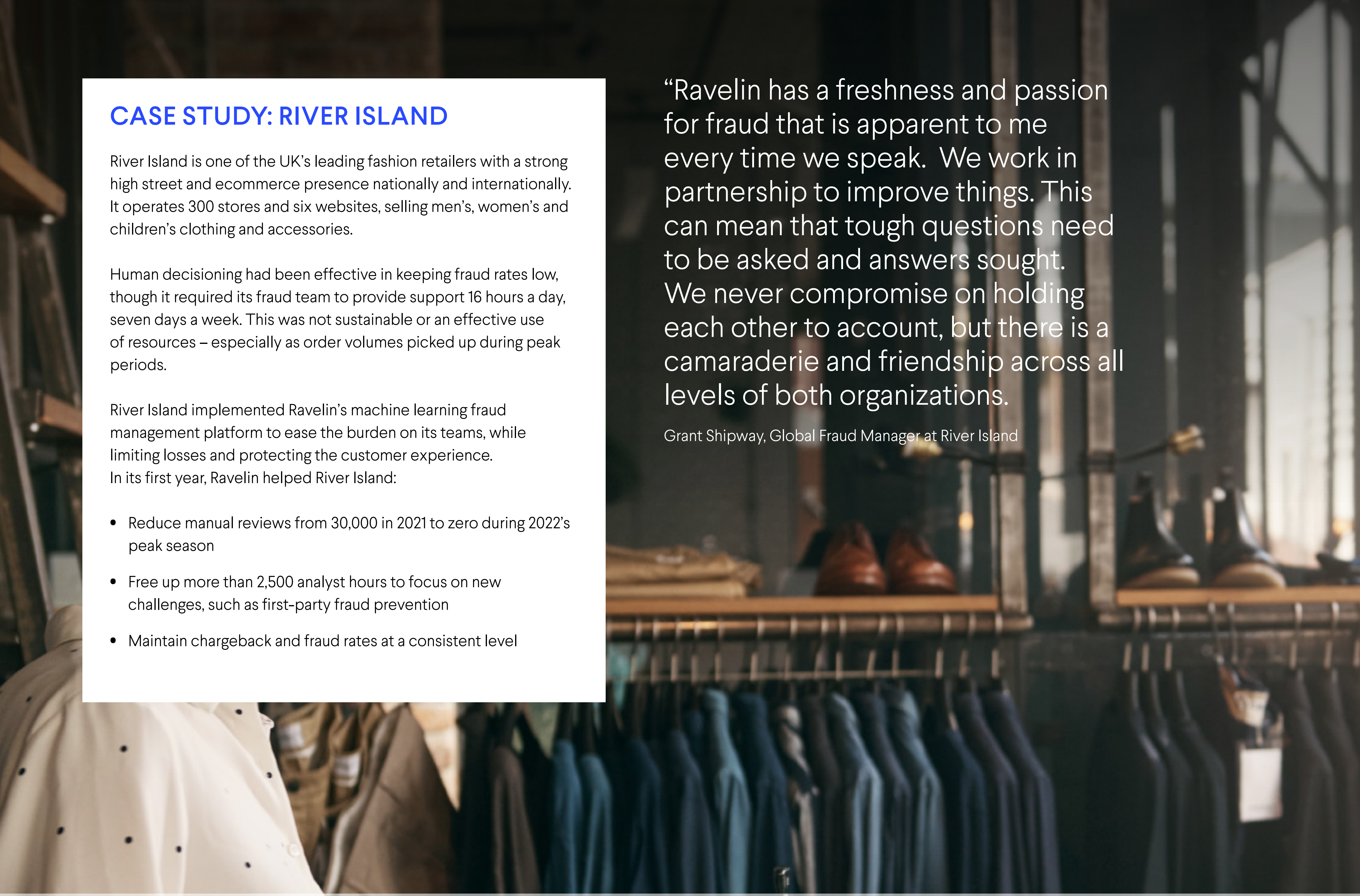
CFOs overwhelmingly believe their fraud teams are well-respected in the business. Over 90% agree their fraud teams' reputations have changed for the better over the past year. A lower, but still respectable proportion, strongly agrees that teams are effective at fighting fraud (57%), protecting the business reputation (62%), and keeping costs down (57%).

CHART 7: How do you expect your fraud management budgets and headcount to change in the next 12 months?



Are these resources being deployed to best effect? Our survey suggests investment in tooling and technology lags behind spending on people. When asked about the nature of the tools and technologies used to support fraud detection and prevention, the vast majority of respondents (80%) say they use either wholly or mostly in-house solutions. In other words, barely a fifth make heavy use of outsourced, best of breed platforms.

For businesses like retail, which are highly seasonal in nature, a dependence on human intelligence could lead to oversights and low morale at peak times, when fraud risks are likely to be at their highest. As the case study on the next page explains, machine learning tools can bring speed and scale to human fraud teams - automating investigations, freeing up resources to support more complex fraud, and boosting team morale - all while keeping fraud losses at low levels.



CASE STUDY: RIVER ISLAND

River Island is one of the UK's leading fashion retailers with a strong high street and ecommerce presence nationally and internationally. It operates 300 stores and six websites, selling men's, women's and children's clothing and accessories.

Human decisioning had been effective in keeping fraud rates low, though it required its fraud team to provide support 16 hours a day, seven days a week. This was not sustainable or an effective use of resources – especially as order volumes picked up during peak periods.

River Island implemented Ravelin's machine learning fraud management platform to ease the burden on its teams, while limiting losses and protecting the customer experience.
In its first year, Ravelin helped River Island:

- Reduce manual reviews from 30,000 in 2021 to zero during 2022's peak season
- Free up more than 2,500 analyst hours to focus on new challenges, such as first-party fraud prevention
- Maintain chargeback and fraud rates at a consistent level

> "Ravelin has a freshness and passion for fraud that is apparent to me every time we speak. We work in partnership to improve things. This can mean that tough questions need to be asked and answers sought. We never compromise on holding each other to account, but there is a camaraderie and friendship across all levels of both organizations.
>
> Grant Shipway, Global Fraud Manager at River Island

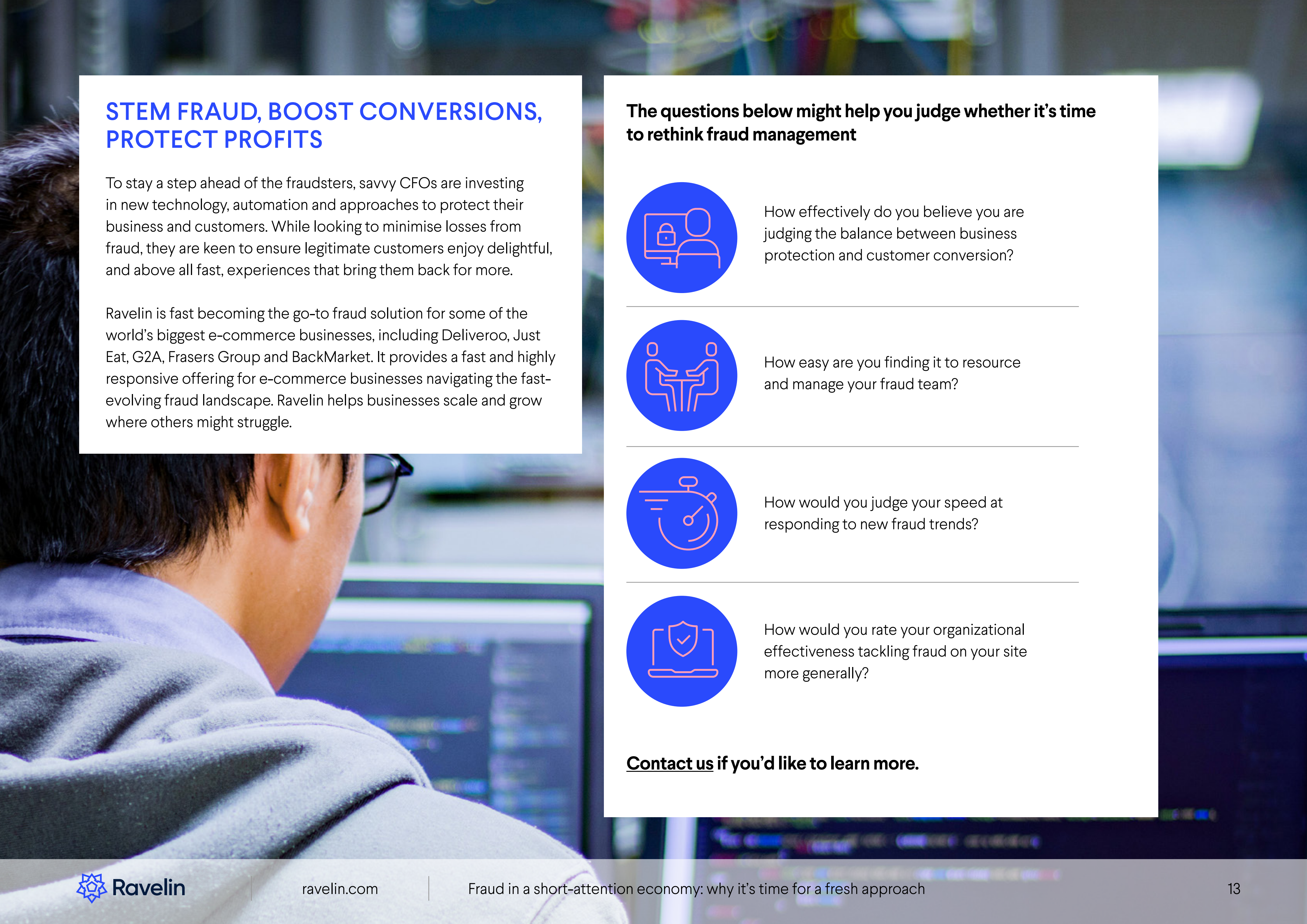
IMPLICATIONS FOR FINANCE LEADERS

There's a fine line between stopping fraudsters and providing a frictionless experience for everyone else to drive growth.

The rise of the professional fraudster and increased opportunism on the part of consumers suggest that throwing increasing spending and hiring more people is an unsustainable strategy. Unrelenting workloads can sap morale, while hiring talented fraud investigators is becoming increasingly difficult.

Finance leaders should look to scale up their fraud capabilities through automation, shifting from rules-based systems to machine learning platforms such as Ravelin. These tools are trained to identify potential anomalies in the day-to-day flow of transactions, without the need for predefined rules. They can green-light, block, or refer for authentication within milliseconds. Legitimate customers see no difference to their experience, while fraudsters are more likely to be caught.

Automating day-to-day fraud management can free up in-house fraud teams to support the business in other areas. These include addressing profit erosion, new product development, and evaluating new payments methods.



STEM FRAUD, BOOST CONVERSIONS, PROTECT PROFITS

To stay a step ahead of the fraudsters, savvy CFOs are investing in new technology, automation and approaches to protect their business and customers. While looking to minimise losses from fraud, they are keen to ensure legitimate customers enjoy delightful, and above all fast, experiences that bring them back for more.

Ravelin is fast becoming the go-to fraud solution for some of the world's biggest e-commerce businesses, including Deliveroo, Just Eat, G2A, Frasers Group and BackMarket. It provides a fast and highly responsive offering for e-commerce businesses navigating the fast-evolving fraud landscape. Ravelin helps businesses scale and grow where others might struggle.

The questions below might help you judge whether it's time to rethink fraud management

How effectively do you believe you are judging the balance between business protection and customer conversion?

How easy are you finding it to resource and manage your fraud team?

How would you judge your speed at responding to new fraud trends?

How would you rate your organizational effectiveness tackling fraud on your site more generally?

Contact us if you'd like to learn more.

ABOUT RAVELIN

Ravelin provides technology and support to help online businesses prevent evolving fraud threats and accept payments with confidence. Combining machine learning, graph networks, behavioral analysis, and expert rules, Ravelin helps businesses draw deeper insights from their customer data to detect fraud, account takeover and promotion abuse, and increase payment acceptance. www.ravelin.com