THE BALANCING ACT

Minimise Fraud. Minimise Costs. Maximise Revenue.

2016 UK eCommerce Fraud Report

CyberSource®

To minimise fraud losses, you need to reduce the number of fraudulent transactions going through your systems. And to maximise revenue you need to ensure that genuine orders are able to be recognised and processed easily and speedily. All this while you're making sure your operational costs are kept to the minimum.

Managing fraud effectively requires the balancing of all three areas, which in an increasingly complex environment can be difficult to achieve.

Our latest survey of UK businesses indicates that fraud teams need to achieve this difficult balancing act without more budget or any reduction in pressure to deliver results.

Because of this, the report not only looks at trends and challenges facing UK fraud managers as reported in our survey, it also discusses approaches and tools available to help you to respond.

ABOUT THE SURVEY AND RESPONDENTS

We commissioned an in-depth survey of 200 UK businesses to gain insight into their challenges and priorities for managing eCommerce and mCommerce fraud. Based on the results, this report summarises the key findings.

This survey was carried out during September 2015, and was conducted in conjunction with Vanson Bourne a leading independent specialist in market research for the technology sector.

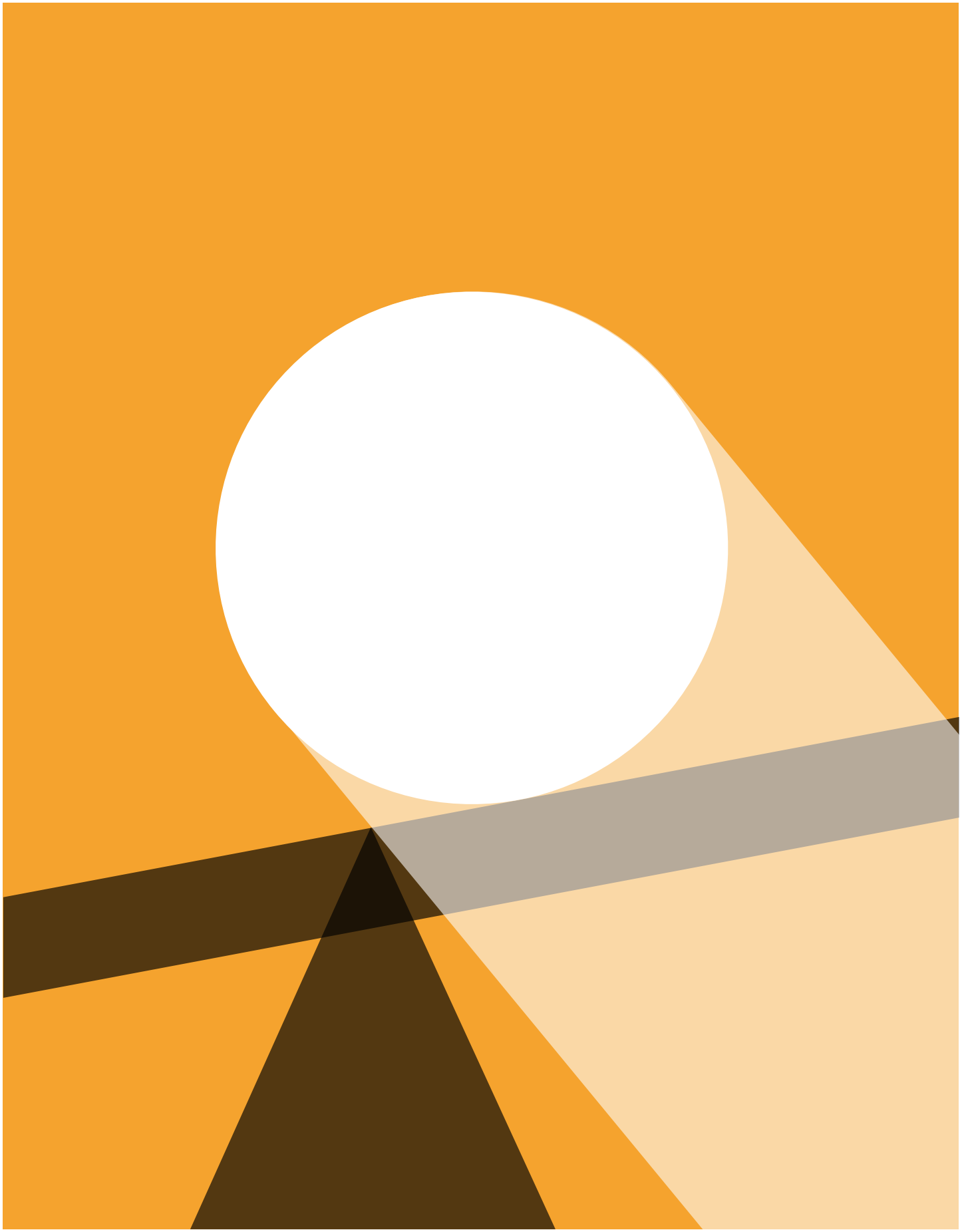
Respondents by Market Sector

- 26% Physical goods
- 23% Digital goods & event tickets
- 23% Services, excluding travel
- 17% Travel
- 11% Subscription services

Size of Business by Estimated 2015 eCommerce Revenue

- 10% Less than £500,000
- 30% £500,000 – £5m
- 30% £5m – £25m
- 30% More than £25m

For the purpose of this survey, our eCommerce definition includes orders placed via webstore, mobile, tablet and telephone. Specific questions related to mCommerce include orders placed via mobile and tablet devices only.



1. LEARN TO FIND THE RIGHT BALANCE

BALANCED FRAUD MANAGEMENT CALLS FOR OPTIMISED FRAUD OPERATIONS

Looking at the respondents' main fraud management challenges and their priorities for the next 12 months, it's clear that the balancing act looms large for them.

FRAUD ITSELF IS UNDER CONTROL

Losing revenue to fraud is fifth out of the six challenges asked about, and improving chargeback management is fifth of six priorities.

This suggests that UK businesses feel they are largely in control of the traditional centrepiece of fraud management – minimising fraud losses.

BUT THE BALANCE ISN'T YET RIGHT

The top challenge is manual review and the top three priorities all relate to doing it less (using analytics better and improving automated detection) or better (streamlining manual review). This may be because manual review is typically the largest fraud management cost, and can be a threat to the overall customer experience and to revenues if not done well.

The other top challenges are an inability to accurately measure fraud metrics by sales channel, which shows a focus on the omni-channel environment, and the risk of losing too many good customers when trying to detect fraud, which shows a concern with avoiding over-zealous fraud management which can hurt efforts to maximise revenue.

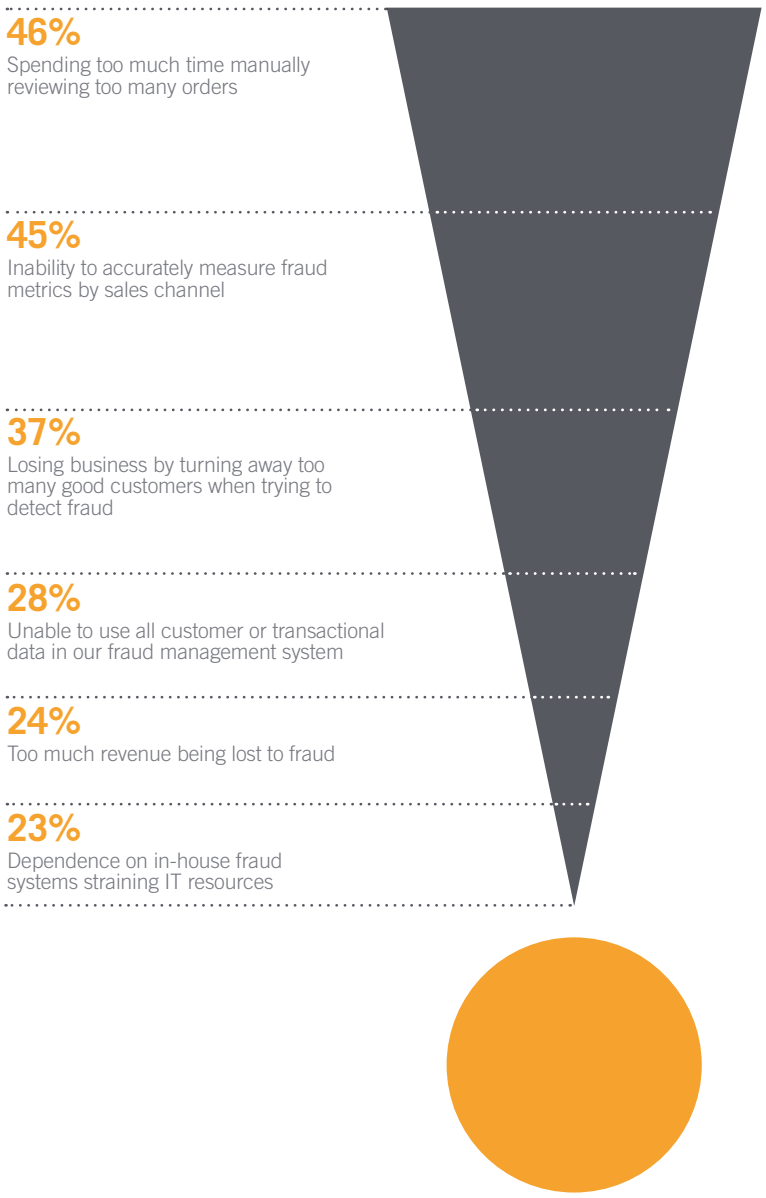
These results highlight that parts of the balancing act (maximising revenues and minimising operational costs) may need more attention.

Base 196.

Respondents could choose 1-3 challenges from 6 options.

Excludes 'don't know' responses.

Fig 1. eCommerce Fraud Challenges Of Greatest Concern



THE FOCUS IS ON OPTIMISING FRAUD OPERATIONS

These results indicate that fraud teams are focused on optimising their fraud operations to do more than achieve low overall fraud rates.

They want to:

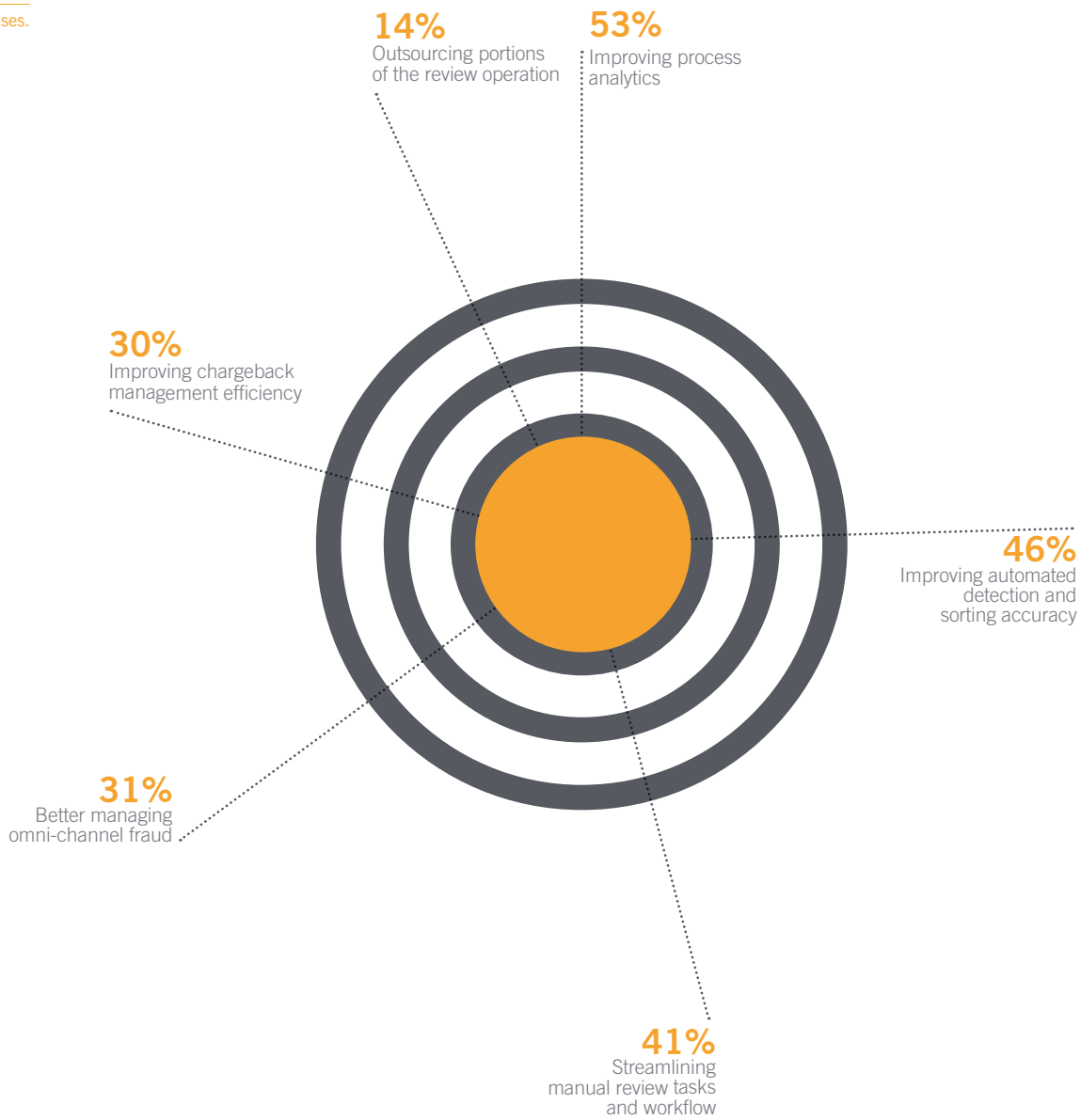
- Be more efficient, especially with regard to manual review.
- Manage fraud better by channel.
- Minimise the risk of turning away good customers.

Base 188.

Respondents could choose 1-3 areas for improvement from 6 options.

Excludes 'don't know' responses.

Fig 2. Priority Areas For Improvement Over The Next 12 Months



2. LEARN WHEN AND WHEN NOT TO REVIEW

OPTIMISING FRAUD MANAGEMENT THROUGH MORE EFFICIENT MANUAL REVIEW

Manual review is typically the largest fraud management operational cost, so it's hardly surprising that businesses want to minimise it – especially when budgets are expected to remain essentially flat as reported by respondents.

FRAUD MANAGEMENT BUDGETS REMAIN FLAT

- On average, 66% expect no change in fraud management budget in the next 12 months.
- Overall, those in the group expecting a change expect an average increase of 3.7% in budget.

With retail eCommerce growth predicted to remain at 10% or above for at least two more years[1], the proliferation of mobile devices and orders[2], increasingly demanding customers and a growing number of data breaches[3] – fraud management teams have the unenvious task of needing to do more with the same.

Base 184.

Excludes 'don't know' responses.

Fig 3. Expected Fraud Management Budget Changes Over Next 12 Months

	Total	Less than £500,000	£500,000 – £5m	£5m – £25m	More than £25m
No change	66%	78%	59%	67%	67%
Average (Mean)	3.71%	-3.00%	3.56%	5.60%	4.10%

[1] http://www.emarketer.com/Article/UK-Retail-eCommerce-Sales-Reach-60-Billion-This-Year/1012963

[2] eMarketer UK Retail eCommerce 2015: Smartphone Shoppers Driving Sales Growth, May 2015

[3] http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html

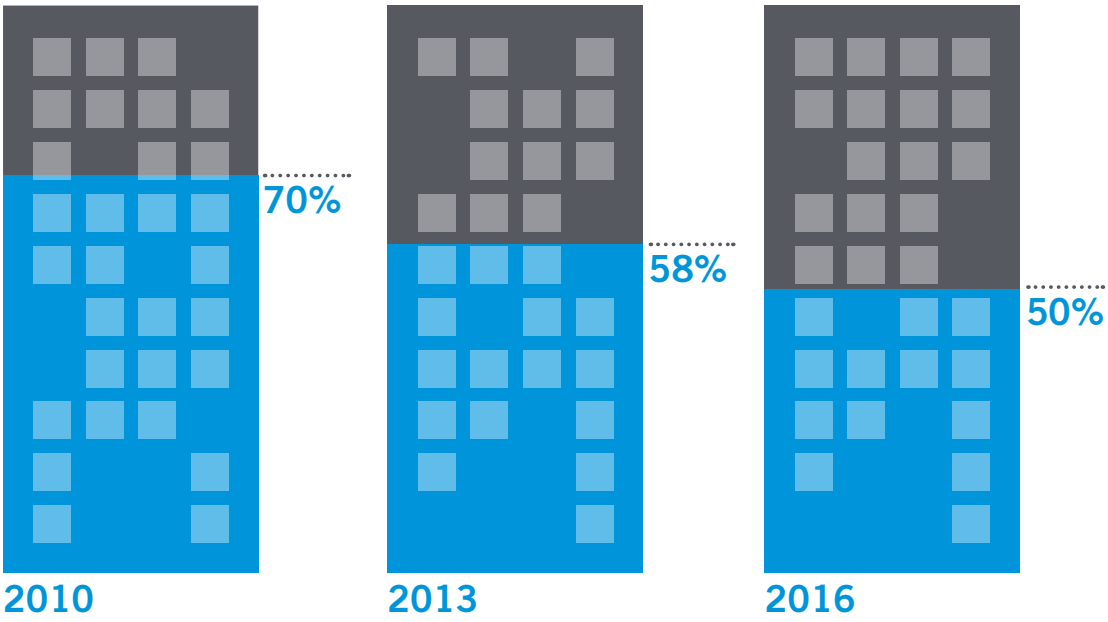
TO REVIEW, OR NOT TO REVIEW

Over the past few years, responses from our UK eCommerce Surveys show that the number of merchants performing manual review has been decreasing, although this year there has been a slight increase. Through working with eCommerce merchants for over 20 years, we understand that some of those businesses not reviewing orders may have well defined automated accept/reject processes.

However, in our experience, the most common reason for businesses not reviewing is that they lack the expertise or resource (or both) to do so efficiently, making them worry that the cost of manual review – both in financial and customer experience terms – will outweigh the benefit.

Manual review can deliver valuable insights to a fraud management strategy. Visibility into fraud patterns and the genuine orders that your fraud screening rules intercept can help fine-tune your fraud rules in order to reduce the level of false positives in your fraud management.

Fig 4. Respondents That Manually Review Orders[4]



Year	% of respondents that manually review orders
2010	70%
2011	64%
2012	61%
2013	58%
2014	No survey held
2015	46%
2016	50%

[4] 2010, 2012, 2013, 2015 CyberSource UK eCommerce Fraud Reports

THE NEED TO IMPROVE MANUAL REVIEW

Respondents reported that:

- 22.5% of orders are manually reviewed for fraud (on average).
- 43% of them are reviewing <10% of orders.
- 5% are reviewing 100% of orders and 14% reviewing at least 50%.

Larger businesses understandably review less, given the challenge of scaling review cost-effectively. Very large businesses are doing better at minimising review, as a larger proportion of them are reviewing <10% of orders, especially compared with the smallest businesses.

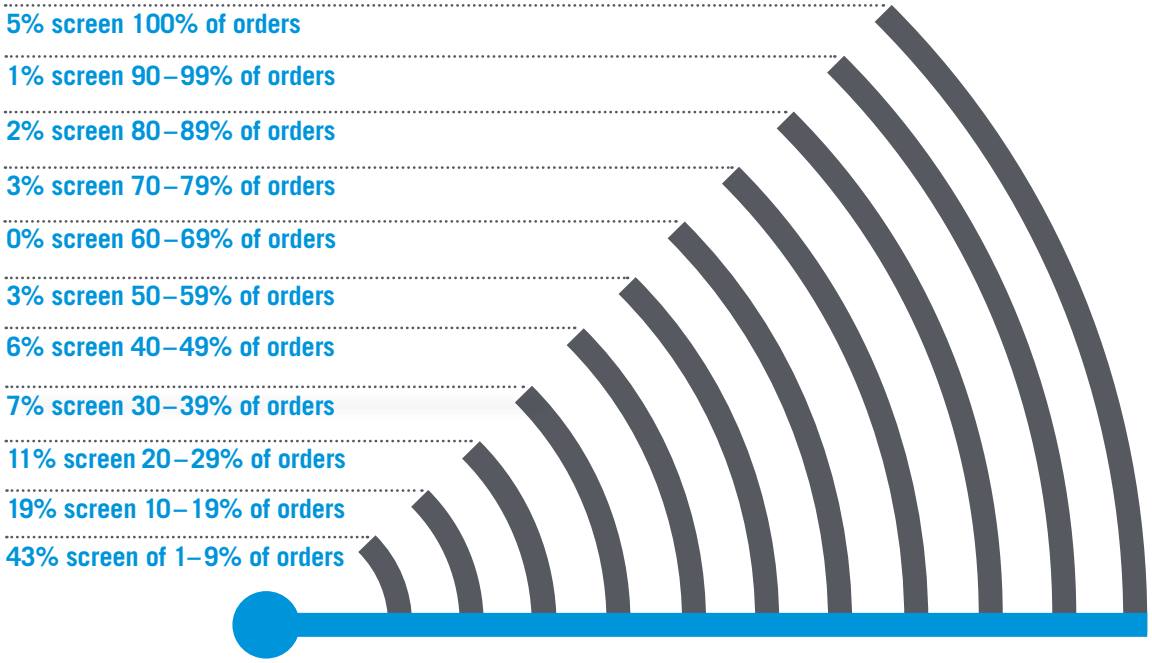
Base 100.

Respondents who review.

Excludes those who do not perform manual review.

Excludes 'don't know' responses.

Fig 5. Percent of eCommerce Orders Manually Screened For Fraud



% of orders manually reviewed	% of respondents			
	Less than £500,000	£500,000 – £5m	£5m – £25m	More than £25m
1 – 9%	22%	39%	39%	57%
10 – 19%	11%	14%	21%	23%
20 – 29%	22%	11%	12%	7%
30 – 39%	22%	7%	6%	3%
40 – 49%	0%	14%	6%	0%
50 – 59%	0%	4%	3%	3%
60 – 69%	0%	0%	0%	0%
70 – 79%	0%	4%	6%	0%
80 – 89%	11%	0%	3%	0%
90 – 99%	0%	4%	0%	0%
100%	11%	4%	3%	7%

BALANCING ACCEPT AND REJECT

Whether a business reviews a little or a lot, the average accept/reject ratio after manual review should be as close to 50:50 as possible (see 'Working Towards a 50:50 Ratio' Learn Zone).

Only 13% of those respondents reviewing are accepting 40–59% of orders, giving them close to a 50:50 accept/reject ratio for manual review. This is a good improvement over last year, when half as many were in this range[5], but it's still a long way from ideal.

The vast majority are either accepting or rejecting the majority of orders they review – more than a third (36%) are rejecting >80% of the orders they're reviewing and almost a quarter (24%) are accepting >80%. Both are a strong sign that a business may be reviewing more than it needs to and could reduce review through more effective automated screening.

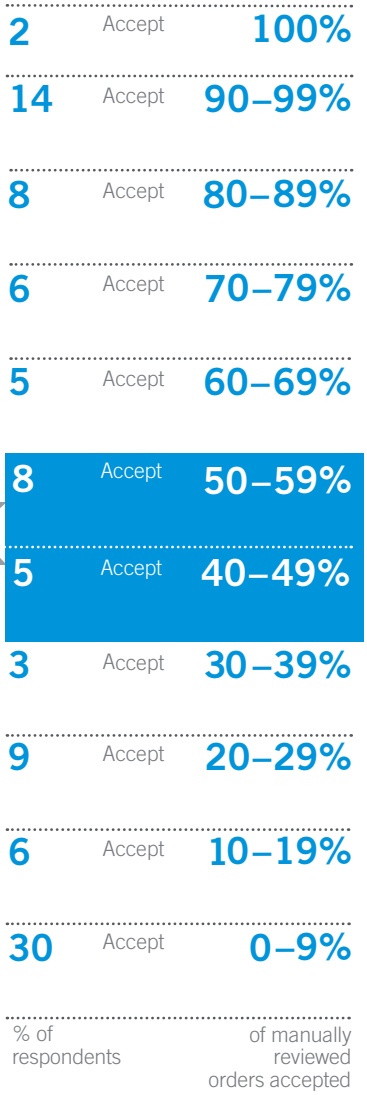
Base 87.

Excludes those who do not perform manual review.

Excludes 'don't know' responses.

4% of respondents 'don't track'.

Fig 6. % Of Manually Reviewed Orders Accepted



LEARN ZONE WORKING TOWARDS A 50:50 RATIO

A 50:50 ratio indicates that review is reserved for orders that really are hard to make a decision about. A ratio far from 50:50, indicating mostly acceptance or rejection of reviewed orders, strongly suggests the presence of factors that could be worked into rules to automate many of these decisions, thereby reducing the amount of manual review required.

Work towards a 50:50 ratio by:

- Analysing the orders that reviewers accept and reject to find common factors (or combinations of factors) being used to make decisions.
- Use this insight and turn it into rules that will automatically accept or reject those types of orders.
- Ensure regular feedback between review and rule-setting to create more comprehensive rules and minimise the amount of manual review required.

[5] 2015 CyberSource UK Fraud Report: Series 2; The Order Acceptance Challenge

AUTOMATE WHAT YOU CAN

- Of those respondents that use automated tools, on average eight automatic tools are used to screen orders for fraud.
- 3% don't use any automated fraud detection tools.

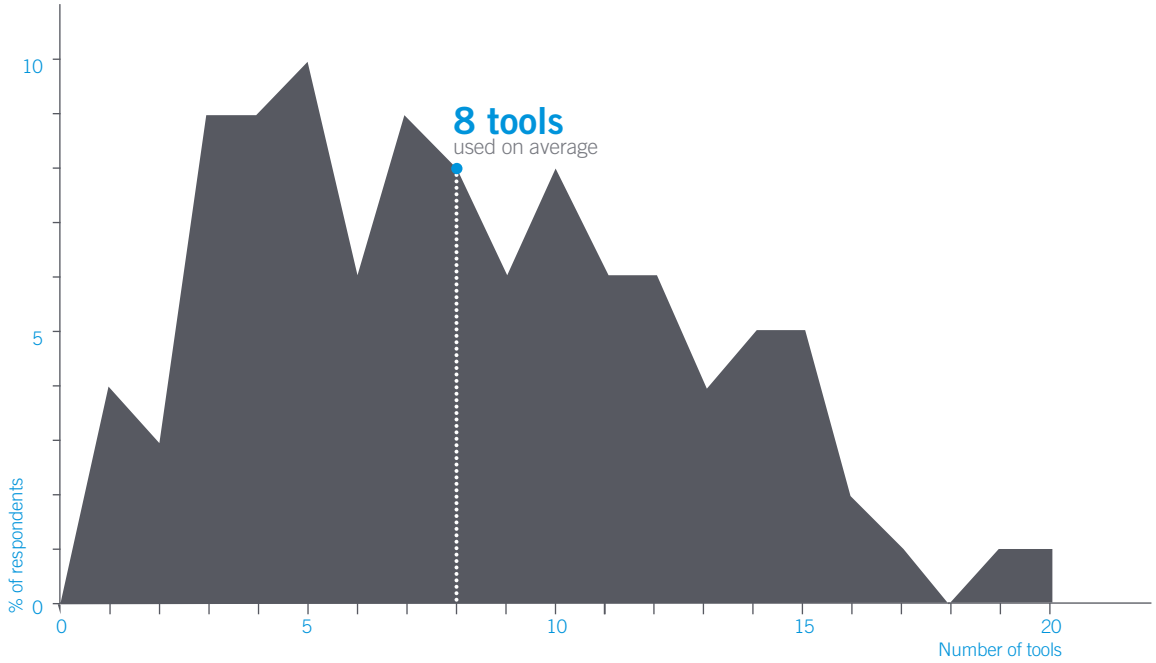
A well-developed automated screening process can deliver rapid, accurate and efficient decisions about the majority of orders, leaving only the most suspicious orders for the review team to investigate manually.

When it comes to effective fraud management, data is key. Whatever the data being captured – basic payment information, device fingerprints or anything else – the value is multiplied many times over by cross-referencing it with other data sources globally, such as feeds of known infected computers, IP geolocation databases and global transaction histories.

Base 200.

Excludes 'don't know' responses.

Fig 7. Number Of Automatic Tools Used To Review Fraud



LEARN ZONE

USE LAYERS TO DEFEND AGAINST FRAUD

The goal of any fraud management strategy is to accurately identify and accept good orders, while keeping fraudsters out. A multi-factored approach, or using a layered set of detectors in concert, can help defend against fraud.

Ask For Reliable Information
Force the fraudster to surrender a key piece of reliable information using hard rules (e.g. disable shipping redirect and require that the shipping address is deliverable).

Add Dimensions Of Related Data
Once you have the key piece of reliable information add 'dimensions' of other, related data that you have on the order (e.g. device fingerprint, account number, email), then build rules using these dimensions in combination.

For example, create rules with shipping address + velocity intervals AND shipping address + account numbers. It makes it more difficult to perpetrate fraud systematically.

Create A Safety Net
In the absence of reliable or available data, use 'generic' information to create a safety net and assess risk based on the level of information you have. For instance, if shipping address information is not available, create rules around risk levels associated with the postcode or shipping address.

STREAMLINING MANUAL REVIEW

Following automated screening, orders that are marked as suspicious may be sent to manual review. Reviewers often use additional data verification sources and apply their own judgement to make a decision.

The sheer volumes of orders being handled by review teams tend to require them to work quickly and efficiently to avoid introducing unacceptable delays into the order acceptance process.

LEARN ZONE

HELP REVIEWERS WORK FASTER AND SMARTER

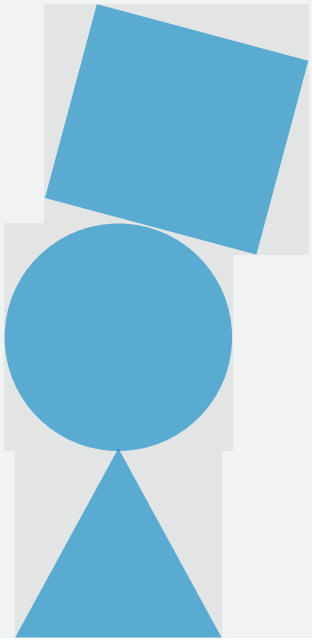
Here are three ways to maximise the efficiency of a review team:

One
Use a case management or review workflow system that:

- Brings together all the relevant order information needed on a single screen, in an easy to understand format.
- Includes links to third-party verification tools such as maps, social media platforms, electoral registers, telephone directories and email domain registers.
- Helps to prioritise orders for review based on criteria such as time-sensitivity (e.g. same-day delivery) or customer profile.

Two
Ensure that your fraud and review teams share knowledge about developing fraud trends. A good feedback loop between analysts and reviewers is vital.

Three
Train reviewers on the differences between channels and markets, and ensure that they understand which information and validation sources work best for each. If your review team is large enough, it may be worth having specialists for certain channels or markets.



IN THE SPOTLIGHT

HANDLING PEAK SEASON

When order volumes increase significantly in a peak period, the review team is put under pressure. Unfortunately, it's not as easy to scale an in-house review team as it is those staffing tills in a store or a customer call centre. Fraud review calls for specific expertise – one of the reasons it's a costly resource. That's why it's unsurprising that a significant portion of our respondents (55%) expect their review staffing to stay the same during peak season. On average, the group expects a small increase in peak season staffing of 3.5%.

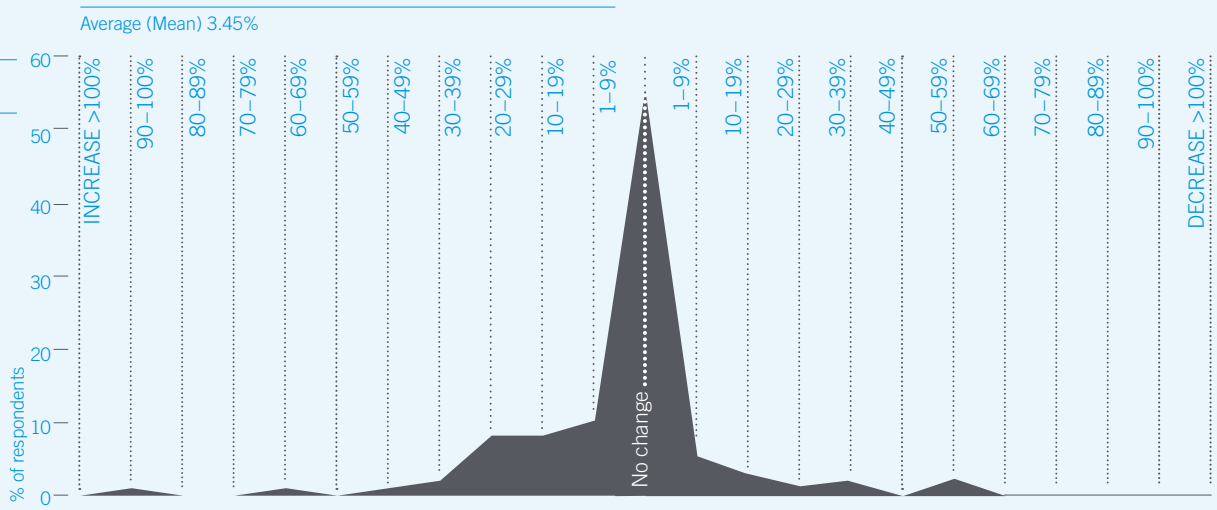
Base 97.

Respondents whose organisation manually screens eCommerce orders for fraud (Fig 5.).

Excludes those who do not perform manual review.

Excludes 'don't know' responses.

Fig 8. Expected Change In Manual Review Staffing During Peak Season



LEARN ZONE — HOW TO PREPARE FOR PEAK

Review Your Historic Data For Patterns
When do your order volumes typically peak? Does fraud often come from a particular geography? Which of your products do fraudsters usually target?

Anticipate Likely New Trends
Based on previous patterns, which new products are likely to be targeted? The hot selling holiday product is often targeted by fraudsters since it is easy and quick to re-sell. And of course, ensure that you're prepared for an increase in mCommerce.

Adjust Your Rules To Match Your Priorities
For example, you may want to plan to relax velocity rules. Also consider the advantages of being able to test potential new rules in advance. As online retailer Backcountry discovered, this can be a real game-changer.

CASE STUDY — HOW BACKCOUNTRY SCALED FRAUD OPERATIONS DURING HOLIDAY SEASON

Backcountry wasn't satisfied with accepting a spike in fraud during peak season, but found it challenging to respond quickly and accurately enough to adjust rules in time.

They implemented Decision Manager Replay, which allowed them to do real-time testing of "what-if" fraud rule profiles against their own historical data.

This gave them added speed and power to test and quantify different fraud strategies in real-time.

This was a game-changer for Backcountry. They could routinely and confidently make rule changes multiple times a week during peak season – helping their fraud defense tactics adapt quickly to rapidly evolving attacks.

As a result they could improve their fraud detection rates during the peak season, even while automating more order decisions and preventing their review team from being overwhelmed.

"Decision Manager Replay was like testing real-time orders faster than real-time."
Jamon Whitehead, Sr. Manager of Payment and Risk Operations, Backcountry.

3. LEARN TO ACT SMART ON THE MOVE

The most unambiguous trend in eCommerce is the growth of the mobile channel. eMarketer stats show that mCommerce accounts for a third of retail eCommerce sales[6]. 59% of our respondents report that they are ready to take advantage of this channel through offering either a mobile-optimised website and/or mobile app*.

mCOMMERCE TODAY

- 59% of respondents support the mobile channel (see Fig 10.).
- 25% of revenue comes through the channel on average (for those who track) (see Fig 9.).
- 21% don't track revenue from orders submitted via the mobile channel.

This survey, which includes travel and event ticket businesses, highlights that mobile accounts for a quarter of eCommerce revenue, for those who track mCommerce revenue. 21% of respondents don't track revenue from orders submitted via the mobile channel.

Unsurprisingly, this average hides sector differences: the average revenue from mobile devices is highest among those buying digital goods, event tickets and subscription services, and lowest for travel bookings.

[6] www.emarketer.com/Article/Mobile-Purchases-Account-Third-of-UK-Retail-Ecommerce-Sales/1012416

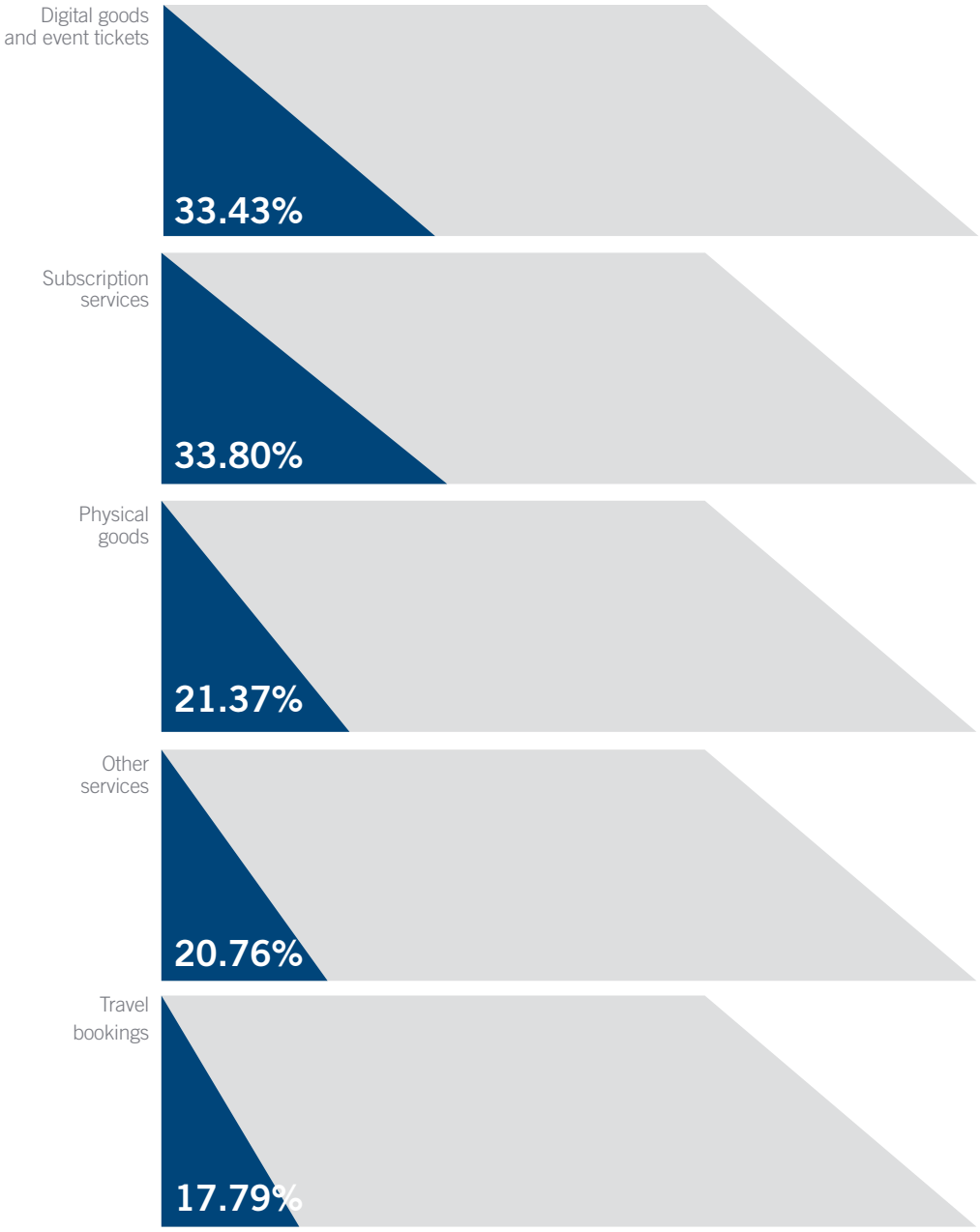
* Question: Which of the following order channels does your organisation have? Respondents could select all that apply, from options Web/online store, Mobile channel (mobile optimised website and/or app), Telephone/call centre or mail order channels, Kiosk, Physical stores.

Base 107.

Excludes 'don't know' responses.

Fig 9. Average % Of Revenue From Mobile Channel, For Those That Track Revenue By Channel

Average 25.07%



YOU CAN'T MANAGE WHAT YOU CAN'T MEASURE

Fortunately most of our respondents realise this: 85% track fraud through their online store; 73% through their mobile channel; 69% through their MOTO* channel; and narrow majorities track fraud in-store and through kiosks, if they have them.

Fig 10.
Base 200.
All respondents.

Fig 11.
Base 198.
Respondents only saw answers previously selected (Fig 10.).
Excludes 'don't know' responses.
10% of respondents 'don't track'.

Fig 10. Order Channels Respondents Currently Offer

100%
Web or online store

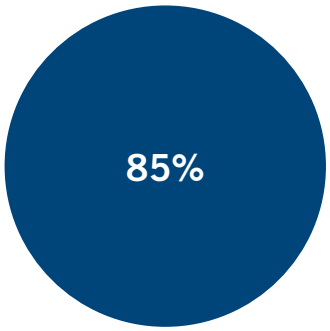
62%
Telephone/call centre or mail order channel (MOTO)

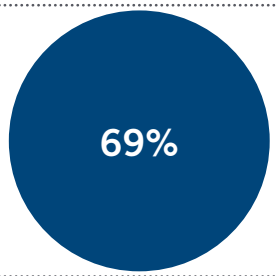
59%
Mobile channel (via mobile-optimised website or mobile app)

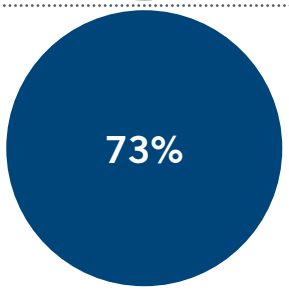
42%
Physical store(s) /face-to-face sales

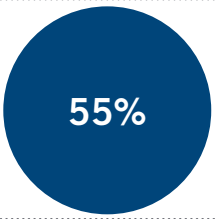
18%
Kiosk

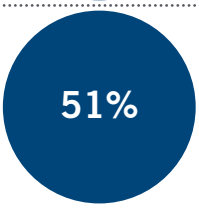
Fig 11. Order Channels Respondents Track Payment Fraud On











* Mail Order and Telephone Order

CASE STUDY — TURKISH AIRLINES MANAGED FRAUD EFFECTIVELY ACROSS CHANNELS

It's important to recognise that a one-size-fits-all approach just doesn't work when managing fraud across channels. Consumer behaviour differs across channels, as does the level of data available.

When Turkish Airlines experienced increased levels of fraud through its call centre, it acted fast to extend its use of our fraud management platform, Decision Manager, and Performance Monitoring service. The airline was already using the platform to help protect its eCommerce channel, but needed channel-specific expertise, which they got in the form of a CyberSource Managed Risk Analyst (MRA).

CyberSource's MRA helped Turkish Airlines define a separate profile for the MOTO* channel within Decision Manager.

By using the same fraud management tool across all its channels, Turkish Airlines were able to respond to fraud in each channel individually, while also identifying and acting swiftly on cross-channel trends and patterns. Soon it was able to cut call centre fraud from 4.4% to 0.01%.

"With the support of CyberSource and our MRA, managing fraud in-house has become a smoother, more strategic process".
Husnu Onur Acemi, Fraud Prevention Analyst at Turkish Airlines

MOBILE: MORE RISKY?

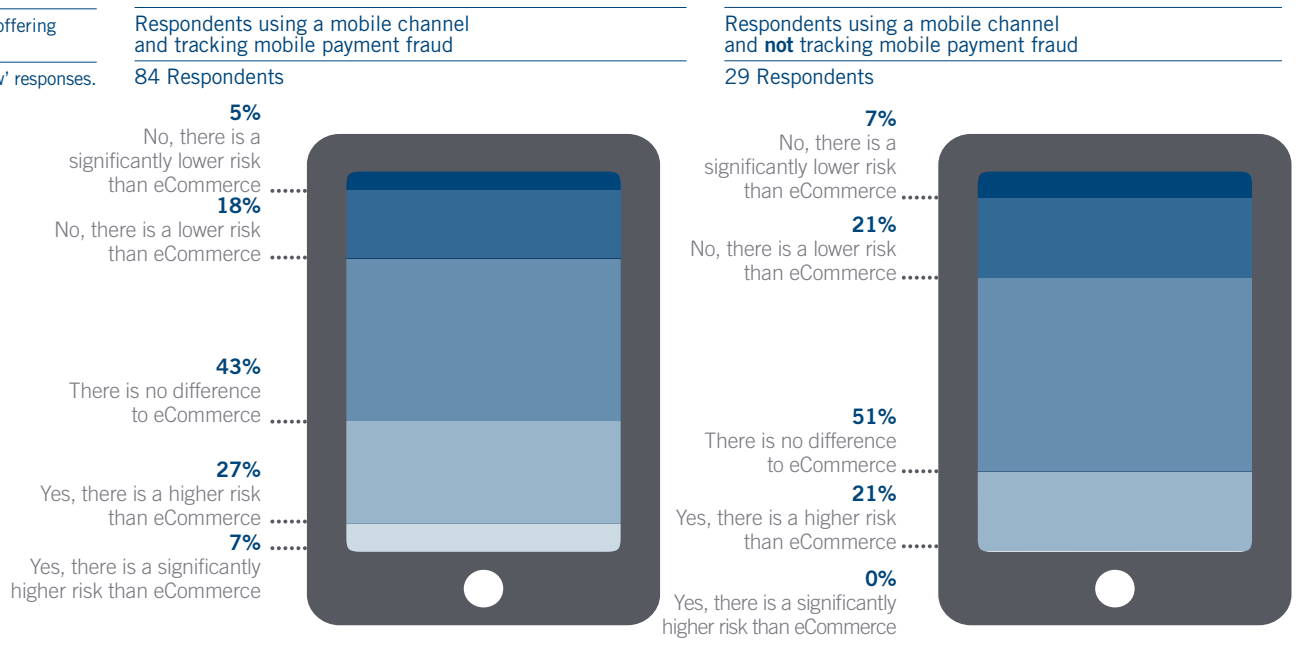
Almost a third of those respondents who support the channel (31%) believe that it is more susceptible to fraud than eCommerce.

There is a difference in perceived risk between those respondents who track the mobile channel for fraud and those who don't.

Those who do track mCommerce fraud are more than 50% as likely to believe it is riskier than eCommerce (34% vs 21% for those who don't track), and also slightly less likely to believe that it's less risky (23% vs 28%).

Base 113.
Respondents who sell through mobile (Fig 10.).
Excludes those not offering a mobile channel.
Excludes 'don't know' responses.

Fig 12. Is mCommerce More Susceptible To Fraud Than eCommerce?



* Mail Order and Telephone Order

CHANNEL DIFFERENCES MATTER

There's no reason that mCommerce should be inherently more risky than eCommerce: the two are just different. They offer different data for fraud management (or the same data is less or more useful) and fraudsters may use different tactics in each. These differences can create the appearance of additional risk. The same applies to call centres, physical stores, mail order: every channel presents unique challenges.

Equally importantly, genuine customer behaviour differs in different channels, and a big part of the challenge of optimising fraud management is to ensure that you're not turning good money away by ignoring this. With mCommerce growing so fast, it's a channel that merits particular attention. The more revenue that comes via the mobile channel, the less you want to risk sub-optimal fraud management endangering that revenue.

THE RIGHT TOOLS FOR THE JOB

89% of respondents use existing eCommerce fraud tools to screen orders that originate from either mobile optimised website and/or mobile app. Typically the same fraud tools can be used, it's just their relative importance that may differ.

LEARN ZONE

BUILD A MOBILE FRAUD STRATEGY

As with eCommerce, the rules created for mCommerce will depend on the data that can be captured, the behavioural patterns and fraud trends that are understood to be relevant, and the level of sophistication that suits your organisation's requirements and risk profile.

It may not be necessary to achieve a high level of sophistication immediately. Here are three simple steps to get started on an mCommerce fraud strategy:

One
Start tracking mobile transactions. Measuring mobile chargeback, rejection and review rates will enable informed decisions to be made about how and when to act.

Two
Create a distinct mobile profile, even if at first the rules applied are an exact copy of existing eCommerce rules.

Three
Start capturing the device type and operating system, even if no rules are immediately implemented, based on the differences in fraud pressure between different devices.

4. LEARN TO RECOGNISE YOUR CUSTOMERS' BEHAVIOUR

When speaking with merchants about their digital commerce growth plans, we find that businesses are understandably keen to avoid anything that may have a negative impact on the customer experience. It's hardly a surprise that turning away good customers is one of our respondents' top three challenges.

GENUINE ORDER REJECTION

Respondents use overall reject rate as a success measure (50%) more than chargeback value (43%).

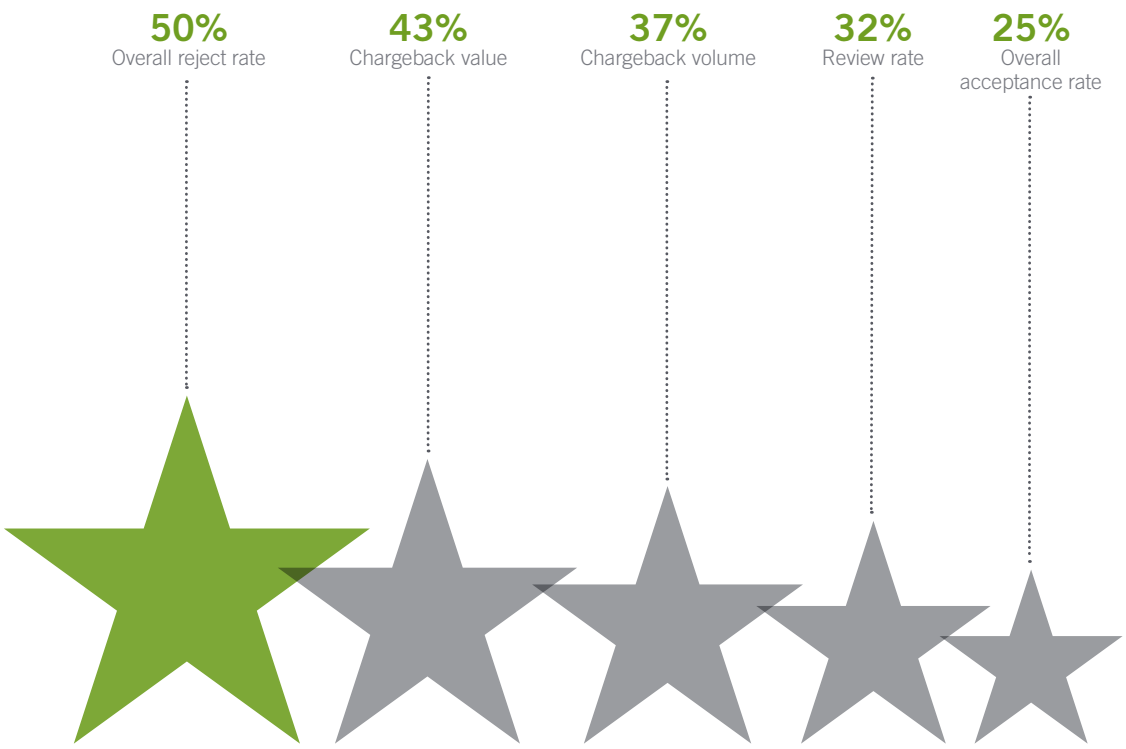
Businesses are generally unhappy with high reject rates because they know that this usually reflects good customers being turned away along with fraudsters.

Base 173.

Respondents could choose 1-3 success measures from 5 options.

Excludes 'don't know' responses.

Fig 13. Primary Fraud-Related Success Measures



WHY GOOD ORDERS ARE BEING REJECTED

Sometimes genuine orders may be rejected if the fraud rules being applied in a particular channel aren't tailored to typical behaviour in that channel.

One of the trends our Managed Risk Analysts have identified is that every year, fraudsters become better at looking like genuine customers, making it harder to distinguish between a good and a bad order.

LEARN ZONE

BUILDING CUSTOMER-CENTRIC RULES

Rules designed to identify genuine orders for automatic acceptance may be transaction-based or customer-based; ideally a mix of both is used:

Transaction-Based Rules
These are based on identifying (from first principles and analysis of historical transaction data) the key pieces of data or patterns that, without any other particular context, create confidence in an order.

Customer-Based Rules
These are based on analysing historical transaction data to build up a picture of what a genuine customer, rather than an order, looks like; then turning that insight into rules.

TOP FRAUD ATTACKS

The two fraud risks respondents indicated they were most concerned about were clean fraud and account takeover, both involve fraudsters having all the information they need to impersonate genuine customers convincingly.

As long as businesses can't confidently distinguish fraudsters from genuine customers, they'll find it difficult to maximise genuine revenue while minimising fraud losses.

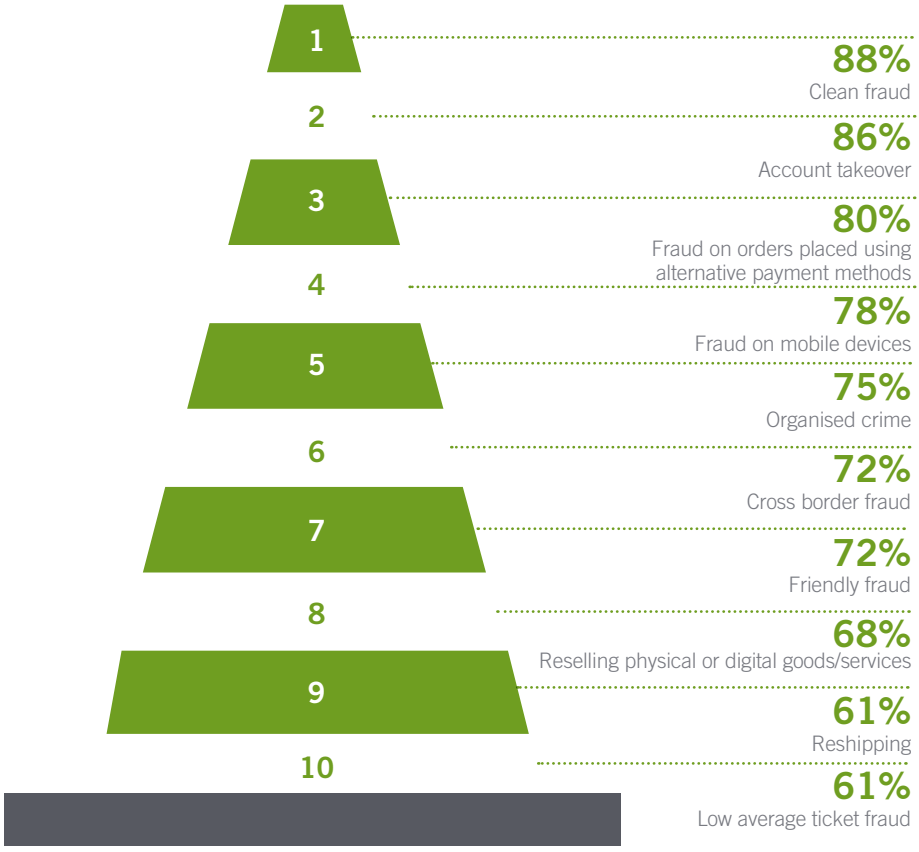
Base 173.

Respondents could select very concerned, somewhat concerned or not concerned.

Excludes 'don't know' responses.

Chart shows combined responses from very concerned and somewhat concerned.

Fig 14. Fraud Risks By Level Of Concern



LEARN ZONE

EXTEND FRAUD MANAGEMENT TO ACCOUNT TAKEOVER

Online fraud management traditionally only happens in relation to payment, but fraud perpetrated through account takeover could potentially be prevented by detecting suspicious account activity before any attempted purchase is made.

To do this, look for a fraud system or service that supports account takeover screening as well as payment fraud management:

One
Just as today you build rules that govern acceptance, review and rejection of purchases, so you should be able to allow, monitor, challenge or block account actions based on rules relating to account creation, login and updates.

Two
You should be able to factor in data relating to usernames, passwords, addresses and devices used.

Three
Ideally you also want to be able to take into account cross-merchant data, and use account takeover decisions to inform your rules for payment fraud detection.

Account takeover screening could be particularly valuable for any business running a loyalty programme. This is especially true in the travel industry, where trillions of loyalty points/miles worth more than 200 billion dollars are as yet unredeemed by the genuine customers who have earned them, making a valuable target for fraudsters[7].

[7] Skift, "Loyalty Program Fraud Can Cost Travelers and Providers a Fortune", Nov 2014

A FULL TOOLKIT

Facing more sophisticated fraudsters who are better armed with clean data, fraud management teams need to step up in sophistication too, using new techniques and tools to distinguish good orders from bad. Our survey suggests that this isn't happening quickly enough:

- Only five of 21 fraud detection tools are used by more than half of our respondents. Three of these – CVN, AVS and postal address validation – may be the most familiar to fraudsters and most easily circumvented with stolen data.
- Many of the tools that are especially valuable in combatting sophisticated fraud are in use by less than a quarter of our respondents. These include two-factor phone authentication, multi-merchant data, and device fingerprinting.

Base 200.

Excludes 'don't know' responses.

Fig 15. Tools Currently Used and Planning To Be Added In Next 12 Months To Assess eCommerce Payment Fraud Risk

		Current usage	Plans for 2017
Validation services	CVN (card verification number – CVC2, CVV2, CID, etc.)	75%	14%
	Address Verification Service (AVS)	68%	20%
	Payer authentication (3-D Secure): Verified by Visa/MasterCard SecureCode/American Express SafeKey	64%	21%
	Postal address validation services	51%	24%
	Credit history check	39%	28%
	Telephone number verification/reverse lookup	39%	29%
	Google Maps lookup	33%	22%
	Paid-for public record services (e.g. Experian, 192business)	32%	28%
	Social networking sites	22%	24%
	Biometric indicators (e.g. voice recognition)	17%	27%
	Two factor phone authentication (e.g. TeleSign)	15%	30%
Your proprietary data/customer history	Customer order history	57%	22%
	Customer website behaviour/pattern analysis	42%	26%
	Negative lists/backlists (in-house lists)	38%	33%
	Fraud scoring model – company-specific	36%	32%
	Positive lists/whitelists	35%	29%
	Order velocity monitoring	29%	23%
Multi-merchant data/purchase history	Multi-velocity/identity morphing models	24%	27%
	Shared negative lists – shared hotlists	23%	34%
Purchase device tracing	IP geolocation information (country, city, etc.)	26%	31%
	Device fingerprinting	18%	31%

LEARN ZONE

INCREASE YOUR TOOLKIT TO COMBAT CLEAN FRAUD

The key to combatting clean fraud is to capture and use additional sources of data that let you go beyond the surface to identify fraudsters and distinguish them from good customers. Here are two examples:

Cross-Merchant Data

Whatever the data being captured, the value is multiplied many times over by cross-referencing it with other data sources globally. No business has direct access to this kind of information, but it is indirectly available through some fraud management systems and services. They will typically use this aggregated data in the base fraud scoring algorithms for your transactions, letting you take advantage of transaction histories that go beyond your own.

Detailed Device Fingerprinting

Fraudsters increasingly sidestep basic device fingerprinting by using proxies to hide their real IP address, and manipulating browser information between transactions to make the transacting device seem different. But a deeper dive can often uncover inconsistencies suggesting fraud, such as a time zone or language setting inconsistent with the location suggested by card details and (spoofed) IP address.

Or you can use a packet inspection service, which can determine whether the transacting device is operating as (or through) a proxy, or has behaviours, such as spamming or firewall scanning, associated with machines under the control of another device.

3-D SECURE PAYER AUTHENTICATION

Respondents report 3-D Secure to be one of the top three tools used the UK to assess eCommerce fraud risk. This is possibly because it's unique among fraud management tools in providing a liability shift for those who use it.

3-D SECURE CAN REDUCE MANUAL REVIEW

While businesses may not be liable for chargebacks on transactions covered by a 3-D Secure programme, they still count towards the fraud scoring used by issuers to create watchlists or impose penalties.

But our survey shows its usefulness as an extra layer of protection in the fact that respondents using 3-D Secure manually review on average almost a third fewer orders (19.86%) than those who don't use 3-D Secure (29.32%).

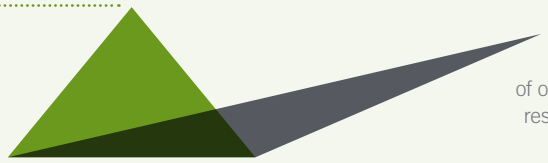
Base 100.

Excludes those who do not perform manual review.

Fig 16. Percentage Of eCommerce Orders Manually Screened For Fraud; Those Using 3-D Secure vs Those Not

AVERAGE RESPONDENTS USING 3-D SECURE MANUALLY SCREEN ONLY 19.86% OF ORDERS

19.86%
of orders are manually screened by respondents using 3-D Secure



29.32%
of orders are manually screened by respondents **not** using 3-D Secure

	Respondents using 3-D Secure	Respondents **not** using 3-D Secure
1 – 9%	32%	11%
10 – 19%	13%	6%
20 – 29%	10%	1%
30 – 39%	5%	2%
40 – 49%	5%	1%
50 – 59%	1%	2%
60 – 69%	0%	0%
70 – 79%	2%	1%
80 – 89%	2%	0%
90 – 99%	1%	0%
100%	1%	4%
Average (mean)	19.86%	29.32%

CONCERNS OVER CUSTOMER FRICTION

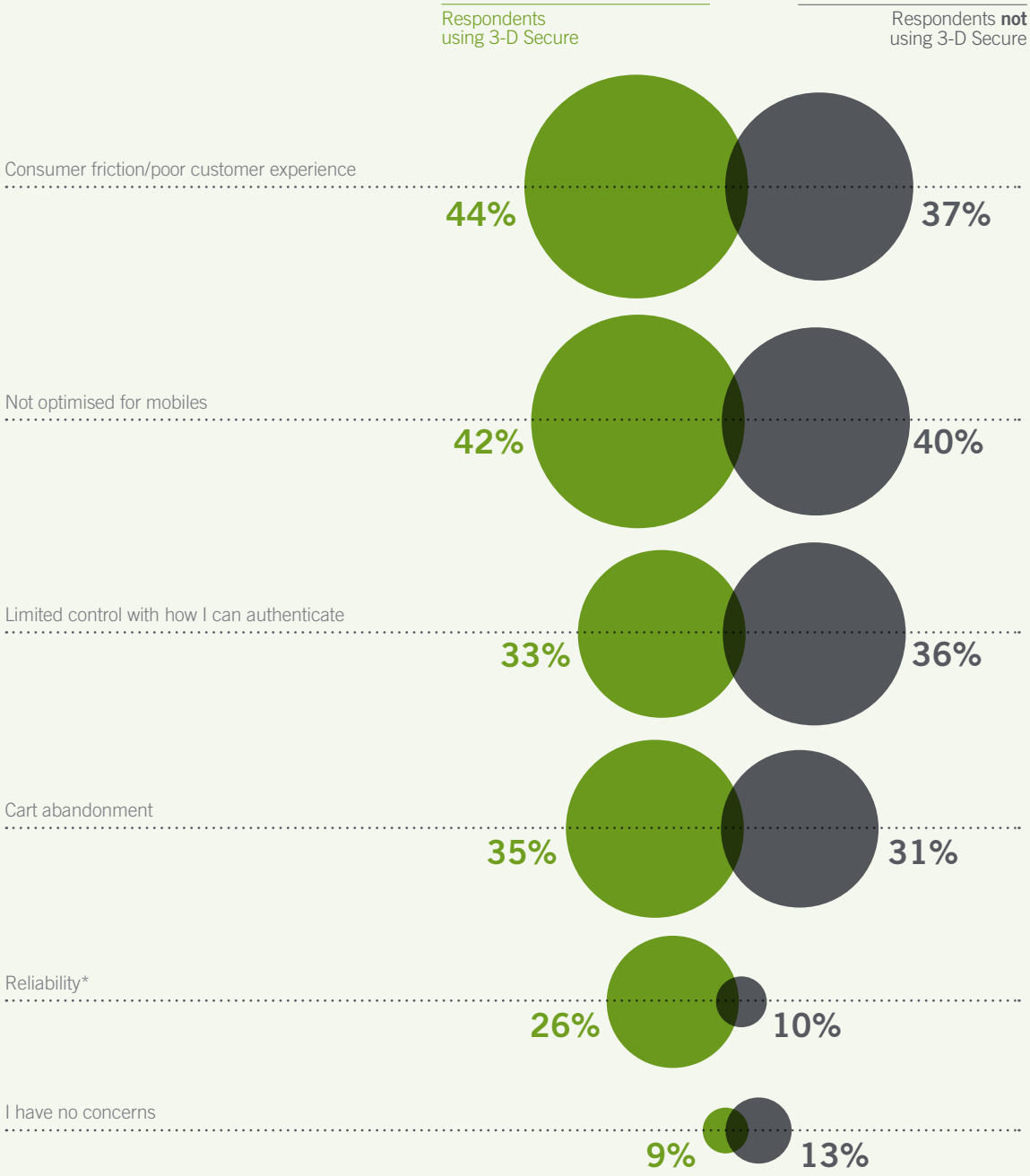
Despite its popularity in the UK, our respondents indicated there are concerns about 3-D Secure. Respondents cite consumer friction (42%), issues in the mobile channel (41%), limited control (34%) and cart abandonment (34%) as concerns.

Reliability can also be an issue, though those not using 3-D Secure tend not to be aware of this as a problem: 26% of those using 3-D Secure cite it as one of their concerns; only 10% of those not using it cite reliability as a concern.

Base 196.

Excludes 'don't know' responses.

Fig 17. Biggest Concerns About Using 3-D Secure



*e.g. latency related to some issuing banks or ACS (Access Control Server) providers

DYNAMICALLY ENABLE 3-D SECURE

Rules-Based Payer Authentication can address many of the concerns around 3-D Secure. This solution gives you control over which transactions go through the 3-D Secure step and which don't.

For example, you could create a rule to disable 3-D Secure for all orders where the card issuer doesn't use risk-based authentication.

These issuers challenge on every order. Knowing this, it may be worth disabling 3-D Secure for these particular orders, while keeping it enabled for most or all other orders (where the risk of a challenge is low).

Rules-Based Payer Authentication provides the flexibility to be very specific about which orders you invoke 3-D Secure for and which you don't.

LEARN ZONE THE BENEFITS OF RULES-BASED PAYER AUTHENTICATION

Rules-Based Payer Authentication allows you to benefit from these advantages of 3-D Secure while controlling the purchase experience.

Improve Margins
- Liability Shift.
- Receive lower interchange rates.
- Minimise chargeback processing costs .
- Authenticate high-risk transactions without manual order review.

Control Authentication Experience
- Choose when to authenticate.
- Avoid unnecessary checkout disruption.
- Embed authentication in checkout.

Increase Conversion Rates
- Reduce checkout abandonment.
- Accept international transactions that require 3-D Secure.
- Let authenticated transactions through.

LEARN ZONE THE EVOLUTION OF 3-D SECURE

Risk-Based Payer Authentication
Issuers are changing the way that they implement 3-D Secure protocols. Transactions are now being evaluated in real-time, with cardholder authentication only being sought on those transactions deemed as medium or high risk. This results in a much smaller proportion of customers being asked to authenticate themselves.

Rules-Based Payer Authentication
Uses real-time issuer level information and transaction information to make an informed decision on the routing of a customer journey. Unlike traditional 3-D Secure it allows for each merchant to select the policy to 3-D Secure that best suits their own business model and requirements.

5. LEARN TO LIVE WITHOUT BORDERS

About three-quarters of respondents (76%) are planning to accept orders from new geographic markets in the next 12 months, and 63% are already serving customers outside the UK.

INTERNATIONAL eCOMMERCE FOR UK BUSINESSES

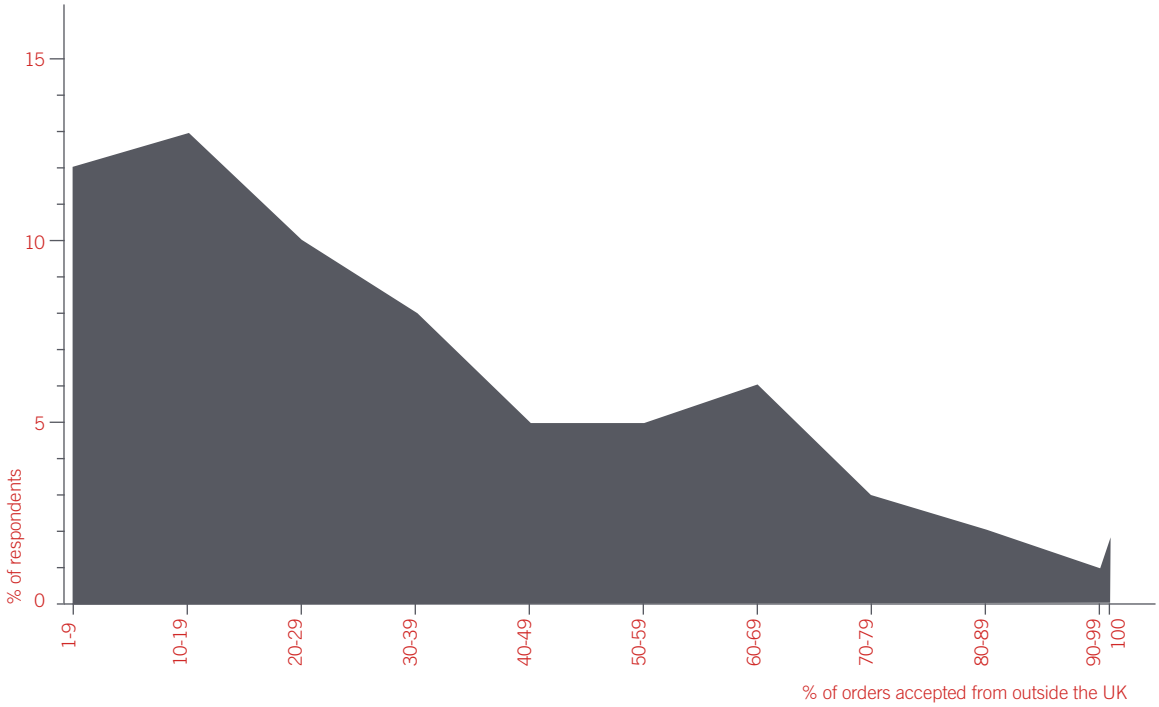
- 76% plan to accept orders from new geographic markets in the next 12 months.
- 63% already accept eCommerce orders from outside the UK.
- On average, of those respondents accepting international orders, 31% of their total eCommerce orders are cross-border.

This means that the majority of our respondents may face a potential problem: the challenge of distinguishing between fraudulent and genuine customers may be exacerbated when serving foreign markets. This is because lack of experience in a new market usually means a lack of knowledge and data about local patterns of fraud and what constitutes normal consumer behaviour.

Base 200.

Excludes those not currently accepting orders outside of the UK.

Fig 18. Percentage of eCommerce Orders From Outside UK



CROSS-BORDER FRAUD CONSIDERATIONS

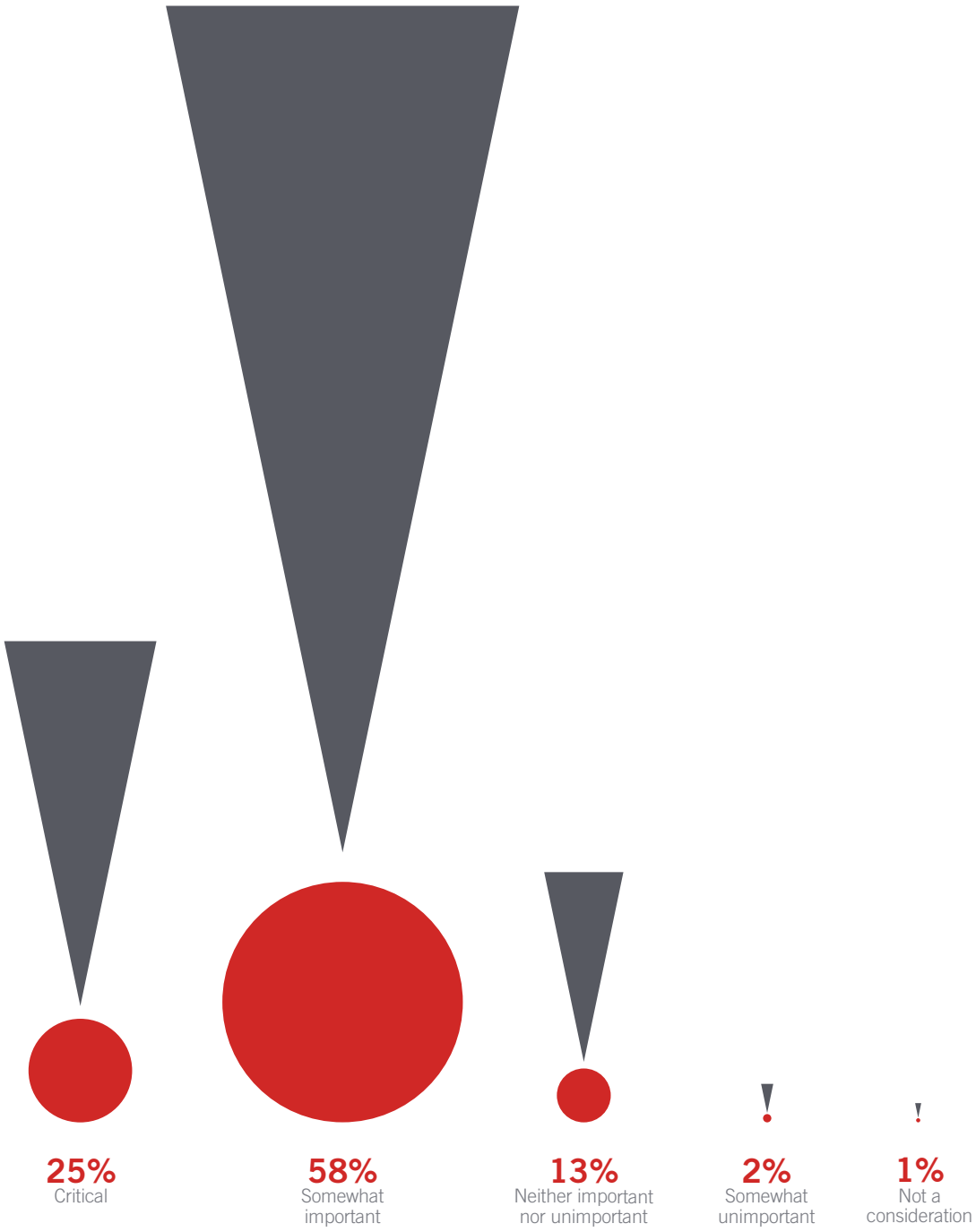
- 62% of those respondents serving foreign markets experience higher fraud rates on cross-border orders.
- 83% of those accepting or planning to accept cross-border orders cite fraud risk as an important factor when deciding whether to accept eCommerce orders from new markets. For a quarter (25%), it's critically important.
- Of those serving foreign markets, 44% block orders at a country level due to high levels of fraud.

Base 163.

Respondents from organisations that accept eCommerce orders from outside the UK (Fig 18.) or plan to accept orders from new markets in the next 12 months.

Excludes 'don't know' responses.

Fig 19. Significance Of Fraud Risk When Looking To Accept eCommerce Orders From A New Market



NO NEED TO BLOCK AT COUNTRY LEVEL

Blocking all transactions from a country is an example of a very blunt rule set. In our opinion it's much better to block at city level or, even better, a specific postcode within a city.

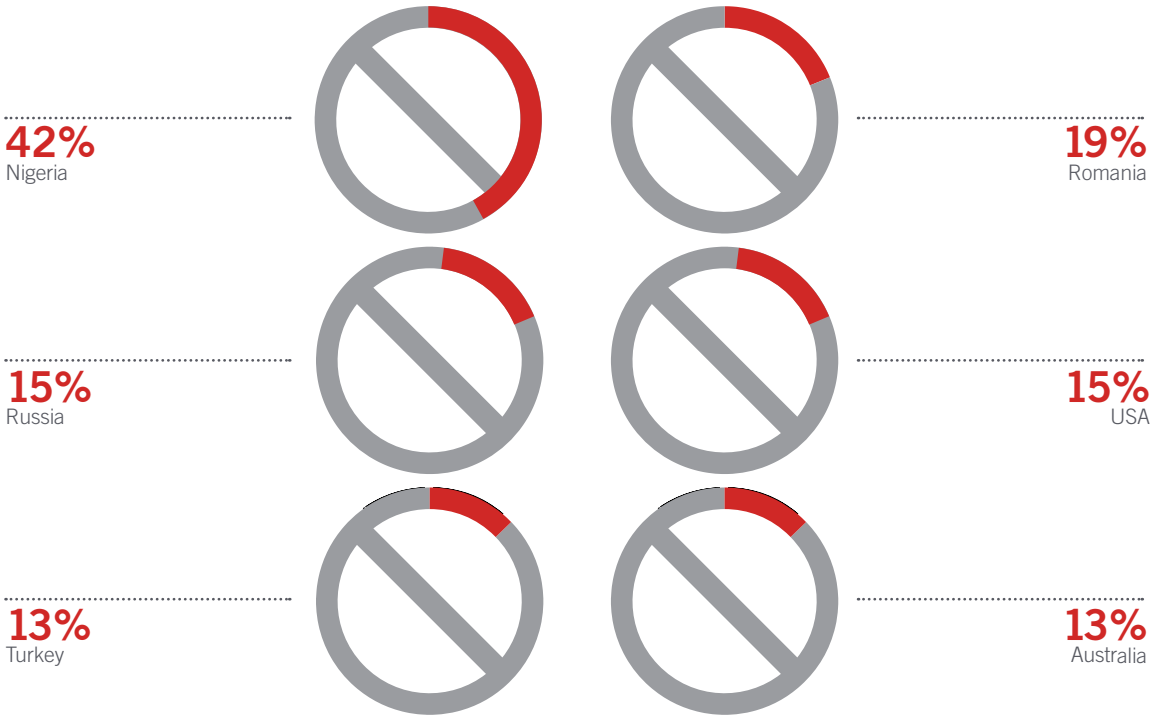
There's really no limit to how intricate the rules can become, to respond to specific patterns from your transaction and chargeback data.

Base 53.

Respondents could choose 1-3 countries from 35 options.

Respondents who have blocked orders at a country level due to high fraud rates.

Fig 20. Top 6 Countries Blocked Due To High Fraud Rates



LEARN ZONE

MANAGING NEW MARKETS

There are two activities merchants should undertake in order to implement effective fraud management rules for orders originating in international markets:

Local Knowledge is Key
You should gain a deep understanding of the fraud landscape in your new market. Local experience and knowledge of fraudster tactics, and genuine customer behaviours, coupled with relevant transaction data, can give you insight into effective rule creation.

One Size Does Not Fit All
You should use a flexible fraud management tool that lets you configure rules for different geographies separately, allowing you to treat your international orders differently from your domestic orders.

CONCLUSION

Of respondents surveyed, 24% ranked losing too much revenue to fraud as one of their top concerns, placing this fifth out of a possible six options, which suggests fraud management is not just about reducing losses from fraud: this should be balanced against the cost to do so, and the effect on genuine business.

Too much manual review can be costly, but eliminating review altogether removes a powerful source of insight and flexibility. Automated fraud screening can be effective and efficient, unless it identifies too many genuine customers as fraudsters. It's a challenging balancing act, and one occurring in an increasingly complex and competitive eCommerce market.

CONSIDER NEW APPROACHES AND TOOLS

As this report has shown, the challenges of fraud management are often addressable. It is possible to reduce fraud losses, operational costs and false positives all at the same time.

Optimised Fraud Management

- Integrates manual review and rule-setting (through analysis and feedback loops) to achieve a near 50:50 accept/reject ratio on manual review for maximum efficiency.
- Gives reviewers sophisticated case management tools to improve their efficiency.
- Takes advantage of iterative 'what if' rules-testing on historical data to quickly and efficiently improve screening accuracy and outcomes.
- Avoids hidden vulnerabilities by working across multiple sales channels while also allowing for strategies tailored to each channel.
- Uses a diverse range of tools – from account screening to device fingerprinting, from customer order history to Rules-Based Payer Authentication – to better distinguish between genuine and fraudulent customers.

Through these approaches and tools, businesses can find and maintain a better balance in fraud management – reducing risk and cost, and actively supporting revenue growth.

HOW CYBERSOURCE CAN HELP

CyberSource provides a complete range of fraud management solutions to help businesses identify fraud faster, more accurately and with less manual intervention.

These include:

Decision Manager
CyberSource Decision Manager is the only fraud management platform that uses data from the World's Largest Fraud Detection Radar, increasing fraud visibility more than 200 times – even for top merchants. With Decision Manager you can create custom rules and models across sales channels and geographies, all on one platform.

Decision Manager Replay
An industry first, Decision Manager Replay enables you to compare various 'what-if' fraud strategies against historical data, producing a real-time report of likely changes to the transaction disposition and fraud rate. You can now confidently quantify the impact of rule changes prior to activating them in the live production environment.

Rules-Based Payer Authentication
Rules-Based Payer Authentication allows you to better control the customer checkout experience, while still benefiting from the secure and effective authentication process of 3-D Secure programs. With Rules-Based Payer Authentication you have the flexibility to determine your authentication experiences for your customers and configure rules to tailor your fraud risk management. You decide when to authenticate or accept liability, which can result in increased revenue, improved margins and decreased fraud.

Account Takeover Protection
Account Takeover Protection defends accounts from fraudulent uses of online accounts and non-payment events, while enabling you to streamline access for valuable returning customers. It can allow you to identify high risk users at account creation and login, and monitors for suspicious account changes so that you can keep your customers' accounts safe.

Managed Risk Services
CyberSource Managed Risk Analysts have deep fraud management experience. Located globally across six continents, our analysts are able to detect the latest fraud trends quickly to help minimise your fraud losses while keeping your operations running efficiently.

For more information please contact us:


+44 (0)118 990 7300


EUROPE@CYBERSOURCE.COM


For a complete list of worldwide offices go to:
WWW.CYBERSOURCE.COM/LOCATIONS

CyberSource®