THE TURNING POINT

OPTIMISE ACCEPTANCE
MAXIMISE PROFIT

CyberSource®
the power of payment

2013 UK eCommerce Fraud Report

INSIDE THIS REPORT

OUR KEY CONTRIBUTORS

Dr Akif Khan

Director, Strategic Initiatives

Akif is a recognised eCommerce industry thought-leader. He advises businesses the world over about payment, fraud and payment security best practices, and is a regular speaker on the European conference circuit. With an eye on the future, Akif provided much insight into the key trends identified in this report.

James Hunt

Senior Managed Risk Services Analyst

One of our most experienced analysts, James has worked for some of the largest global eCommerce merchants across multiple fraud disciplines. Speaking with companies on a daily basis, his first-hand experience has proved invaluable, bringing real-world context to the survey results.

WELCOME TO THE 9TH ANNUAL UK eCOMMERCE FRAUD REPORT

In my time at CyberSource, I've seen online commerce change beyond all recognition. Today, we approach a new era; a truly connected, digital world, with the consumer in the driving seat – looking for a safe, seamless, eCommerce experience, irrespective of device or location.

Our latest report reflects this evolution – we focus on providing you with the tools and insight to accept more customers, faster and more profitably. We explore more channels, including mobile, and markets; with guidance on how you can best optimise the customer journey, and ultimately, your eCommerce expansion.

I hope you find the report beneficial, and look forward to your feedback.

Simon Stokes
Managing Director EMEA, CyberSource

View and download the 2013 UK eCommerce Fraud Report at cybersource.com/ukfraudreport

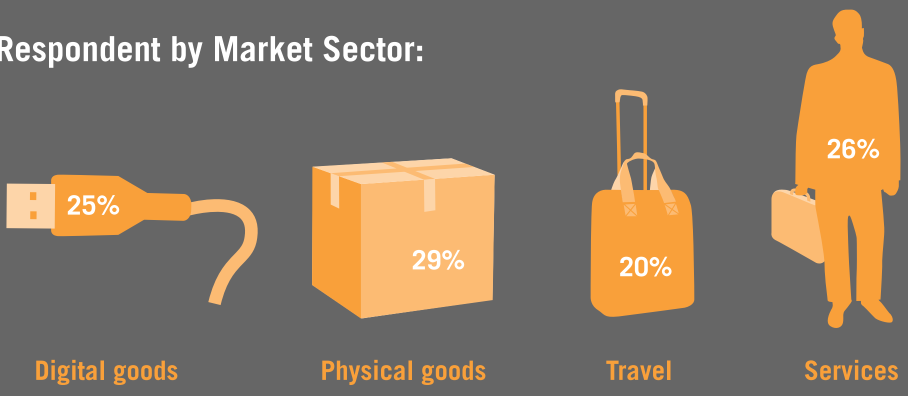
01 | eCOMMERCE TODAY

BEHIND THE SCENES

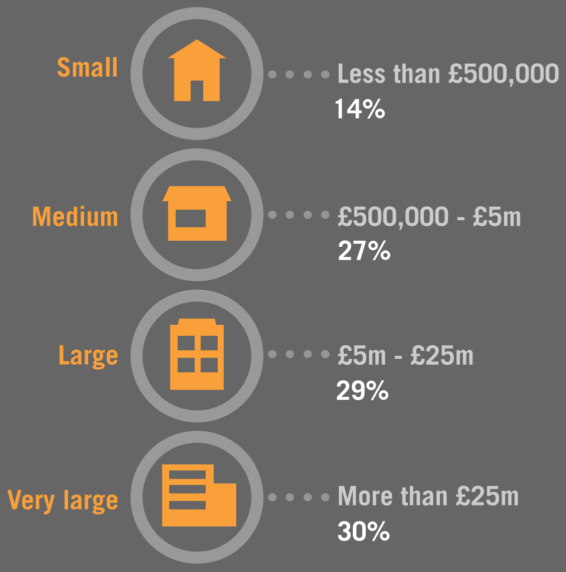
CyberSource's 2013 UK Fraud Report addresses all aspects of UK eCommerce including orders placed via webstore, mobile, tablet and telephone.

We conducted an in-depth survey of 200 merchants across the UK, through our research partner Vanson Bourne, the specialists in technology research. The survey base includes merchants of all sizes and from a variety of sectors.

Respondent by Market Sector:



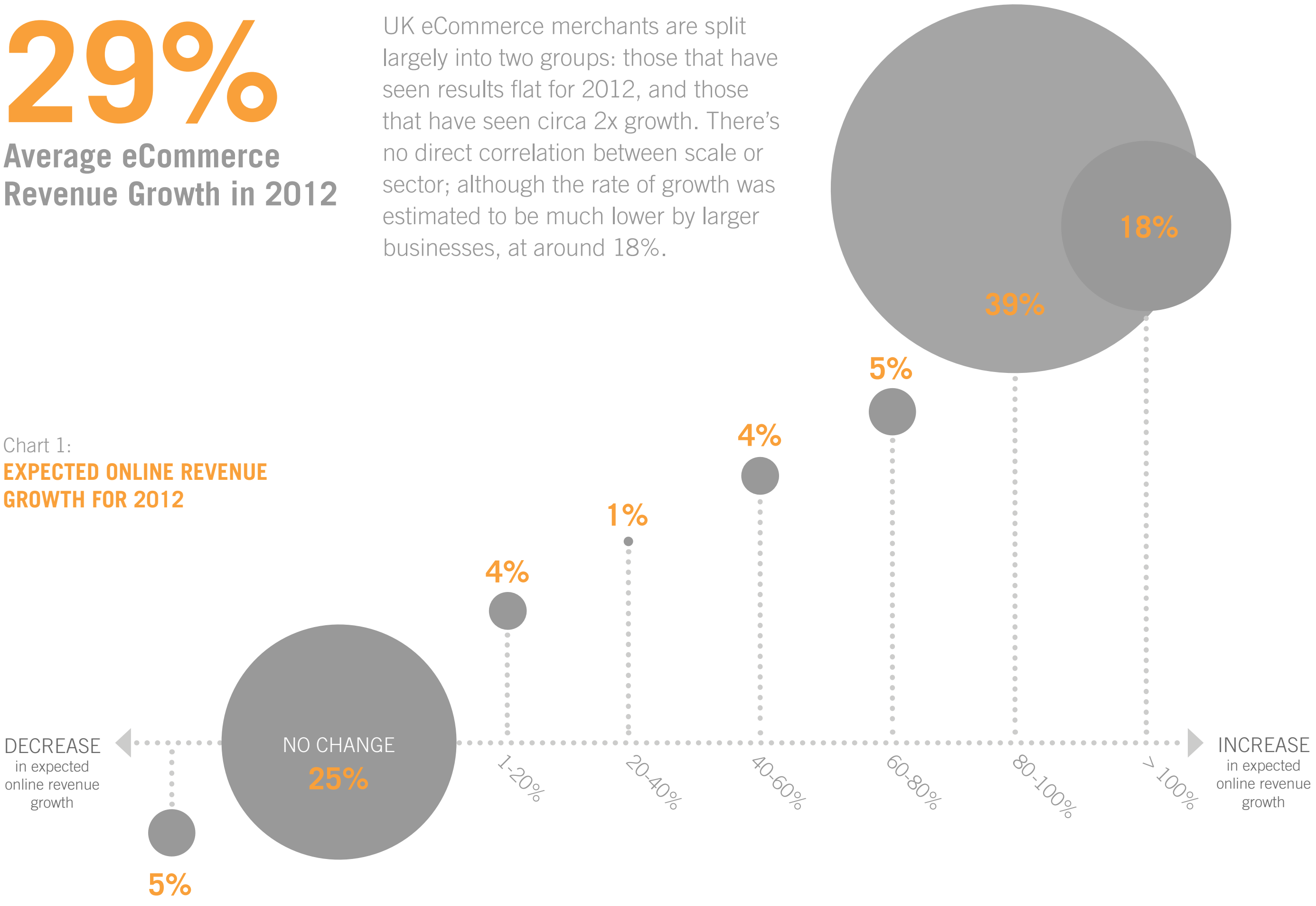
Size of Business by eCommerce Revenue:



29%
Average eCommerce Revenue Growth in 2012

UK eCommerce merchants are split largely into two groups: those that have seen results flat for 2012, and those that have seen circa 2x growth. There's no direct correlation between scale or sector; although the rate of growth was estimated to be much lower by larger businesses, at around 18%.

Chart 1:
EXPECTED ONLINE REVENUE GROWTH FOR 2012



1.65%
of eCommerce Revenues Lost to Fraud

Fraud losses correlate to market sector, with digital goods businesses seeing the greatest loss rate. This could be due to the fact that digital goods are more accessible and have a lower marginal cost. What is more surprising is the small gap between digital and physical goods: physical goods merchants see an average loss rate of 1.89%; this figure will likely have been pulled up by specific respondents.

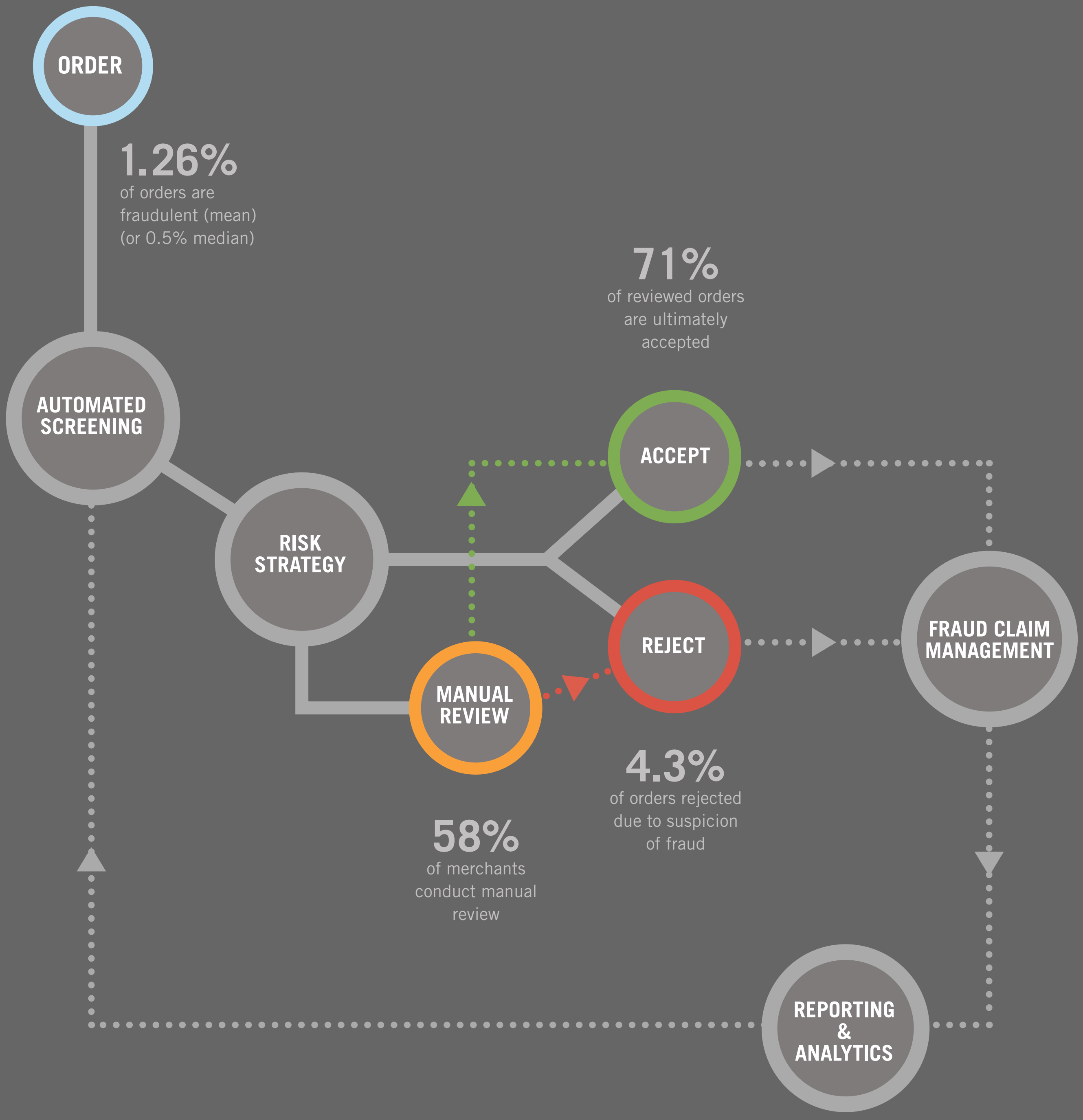
The lowest fraud rates are seen by the travel and services sectors, where offline identity checks are increasingly used to confirm the recipient is genuine (e.g. for financial or identity documents).

LARGE MERCHANTS SPEND HIGHER PROPORTION OF REVENUE ON FRAUD MANAGEMENT

We explored the costs of employing the staff, systems and tools required to manage fraud (excluding actual fraud losses). The results vary significantly; ranging from a median of 5% of eCommerce revenue through to 11% at some organisations.

Larger companies may be allocating more in lieu of the greater threat they face from fraudsters, alongside reputational risk.

02 | FRAUD FUNDAMENTALS



ORDER

1.26%
of orders are fraudulent (mean) (or 0.5% median)

AUTOMATED SCREENING

RISK STRATEGY

71%
of reviewed orders are ultimately accepted

ACCEPT

REJECT

MANUAL REVIEW

4.3%
of orders rejected due to suspicion of fraud

58%
of merchants conduct manual review

FRAUD CLAIM MANAGEMENT

REPORTING & ANALYTICS

How can you identify genuine customers at the earliest opportunity, while sustaining an acceptable fraud level? And how can you keep overheads in line?

With CyberSource’s framework you can assess performance in key areas of your fraud operations: automated screening, manual review, order dispositioning (accept/reject), and fraud claim management. Once you have the foundation, use the results to fine tune operations and increase automation.

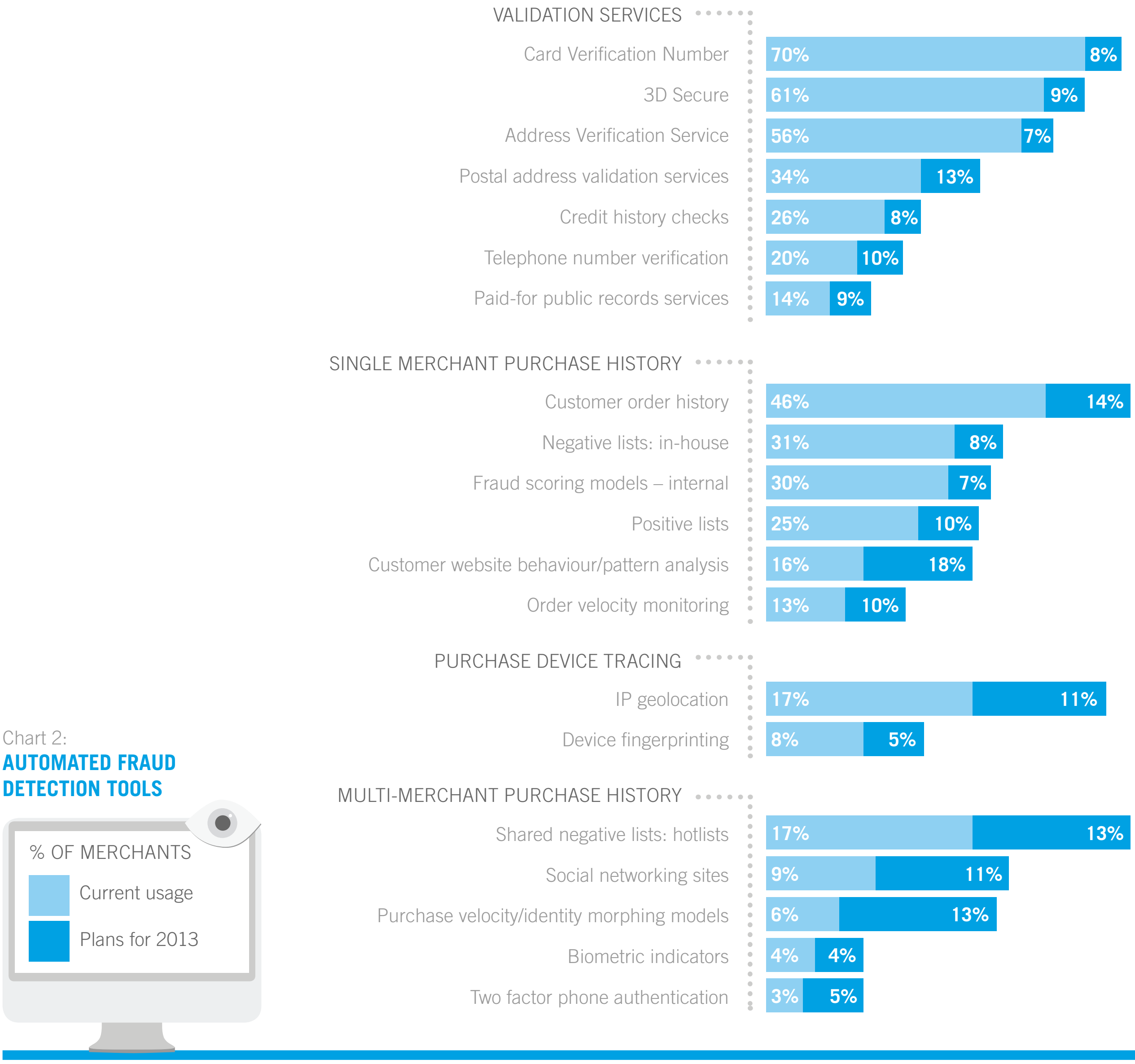
5 FRAUD TOOLS

The Average Used by Each Merchant

The number of tools used varies, with the largest merchants adopting six or more and the smallest, three to four. Significantly, 39% say that one of their greatest eCommerce challenges is the fact that tools are unable to detect the latest fraud threats.

Device fingerprinting usage remains surprisingly low – this is a simple way to improve acceptance rates and recognise returning customers, especially if integrated into a broader screening strategy.

Chart 2:
AUTOMATED FRAUD DETECTION TOOLS



SPOTLIGHT: INVESTMENT PLANNED IN BEHAVIOURAL ANALYSIS

Unlike genuine customers, fraudsters often take a very direct, identifiable route to the checkout, creating recognisable patterns; behavioural analysis can help identify these patterns.

Many merchants will already have some form of analytical software (e.g. Google Analytics) in place on their websites to monitor customer conversion ratios. Metrics like average checkout time and number of webpages visited can be passed to fraud management systems, resulting in more comprehensive profiles for identifying good and bad behaviour.

TAKE ACTION

DEFEND IN DEPTH

- Don't rely overly on one particular anti-fraud strategy or method; you need to use a combination to catch the latest fraud threats;
- Seek guidance from your fraud provider on how to apply tools intelligently, and ensure they can operate via a single connection. Multiple integrations can further impede the overall experience;
- Embrace new tools and old; they evolve, constantly. 3D Secure is one such example, with the migration towards passive authentication.

IMPROVING THE CUSTOMER EXPERIENCE: a Visa Europe Perspective

PETER BAYLEY
SVP FRAUD MANAGEMENT, VISA EUROPE

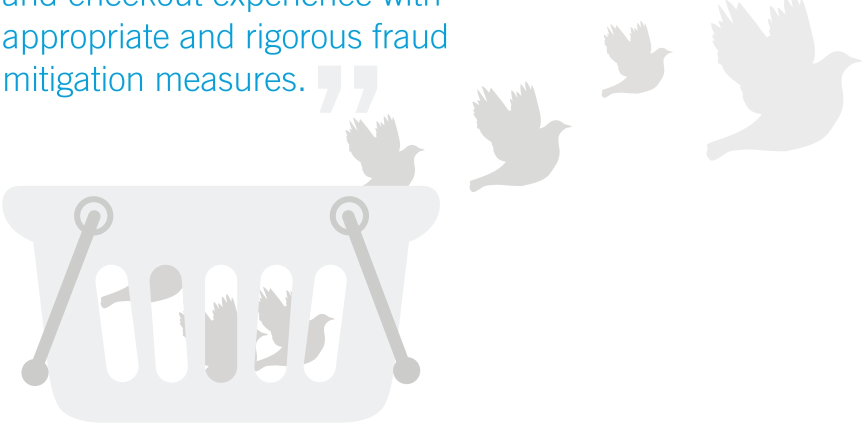
Fraud levels incurred on Visa Europe issued cards remain at historically low levels, reflecting the strong security infrastructure investments made by merchants, issuers and acquirers – notably EMV and 3D Secure.

As such, Visa card payments remain a secure, effective and ubiquitous payment method. The card not present (CNP) channel in particular represents an area of rapid growth for merchants, but the higher risks create increased areas of challenge for all stakeholders to card payments.

Merchants face the challenge of balancing customer acceptance and checkout experience with appropriate and rigorous fraud mitigation measures. Recognising this, Visa Europe continues to create innovative solutions to reduce risk in CNP transactions. Passive 3D Secure authentication has been introduced with issuers starting to approve Verified by Visa authentication without password entry, based on their continually enhanced detection systems.

This results in a smoother customer experience, with increased levels of acceptance on merchant websites, since the challenges associated with password entry are removed in many cases. Verified by Visa on Visa Europe issued cards now occurs for around 50% of all eCommerce transactions, with an authorisation approval rate which significantly exceeds that achieved for unsecured CNP transactions, further helping to increase acceptance levels on merchant websites.

> “Merchants face the challenge of balancing customer acceptance and checkout experience with appropriate and rigorous fraud mitigation measures.”



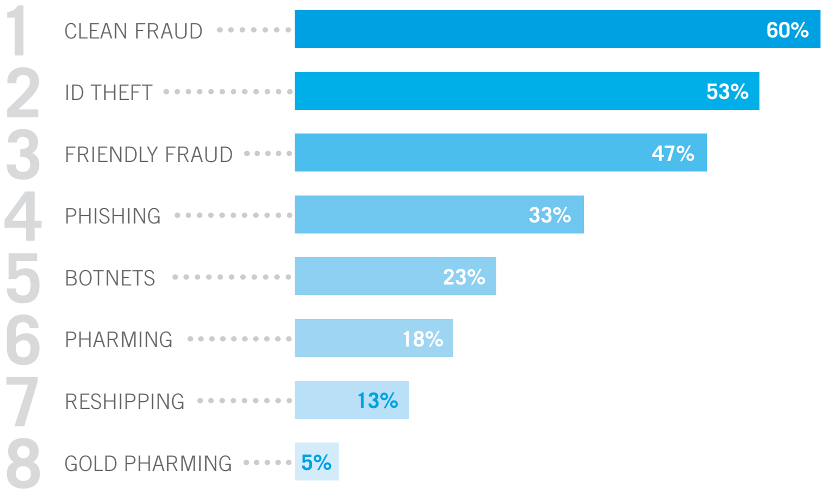
‘CLEAN’ FRAUD

Deemed Biggest Threat; Followed by ID Theft

Digital merchants are particularly concerned about ID theft, while ‘friendly fraud’ (genuine customers subsequently claiming fraud) presents a real challenge to travel businesses. Nearly 60% of respondents to the latest CyberSource US fraud survey said that friendly fraud has increased over the last two years.

CyberSource documented the impact of ‘clean’ fraud some years ago, and it remains a real concern. Ever more sophisticated fraudsters are supplying seemingly complete and correct payment information, making detection difficult.

Chart 3:
FRAUD THREATS OF GREATEST CONCERN



TAKE ACTION

PRIORITISE CLEANER FRAUD

The only way to truly tackle clean fraud and friendly fraud is to address factors outside of ‘classic’ payment data and use tools such as account registration, device fingerprinting, historical and behavioural analysis.

We recommend you take the following additional steps to help address cleaner fraud:

- Use social media to confirm a customer’s location or their behaviour around the time the order was placed, and whether they even exist;
- Check the age of the customer’s email address: Even if the name is in the email address and it appears ‘genuine’, if the address is only a couple of days old it may not have been created by the cardholder;
- Use internet search engines: Planning permission proposals are readily available online and can tie a genuine customer to an address they may not have otherwise been associated with;
- Use the electoral roll: Has the customer previously been registered at the address they’ve provided? If so how long ago and where is their current address? This could be a warning sign of identity fraud;
- Undertake regular data analysis, not just chargeback analysis: Have you seen an increase in the number of orders going to a particular postcode in the last few days, or a rise in interest for a particular product or service which seems unusual?

James Hunt
Senior Managed Risk Services Analyst, CyberSource

1/4 ORDERS

Reviewed by Merchants

58% of respondents manually review transactions, down from 61% in 2012; 7% analyse every order (generally smaller merchants with lower order volumes).

Whilst this step can be an important part of an overall screening strategy, it is essential to reduce the number of orders submitted for review.

48%

of Very Large Merchants have Eliminated Manual Review

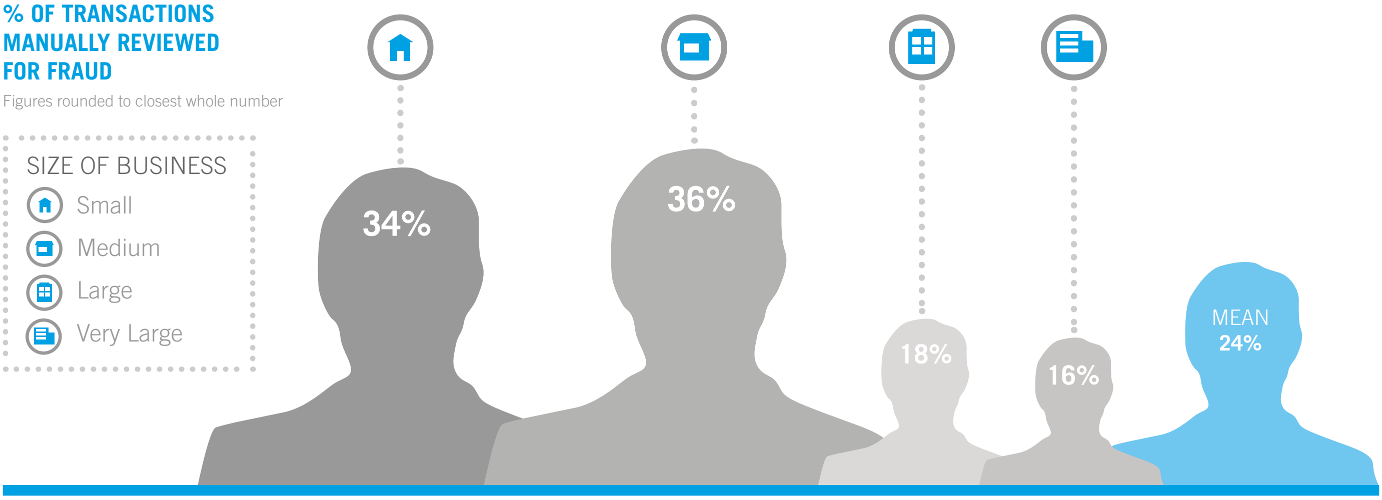
The largest merchants are making strides to eliminate the review process, with many now relying purely on automated screening.

Of those merchants that do perform review, larger companies analyse a much lower proportion. This is expected given the scalability and cost challenges associated with review.

Chart 4:

% OF TRANSACTIONS MANUALLY REVIEWED FOR FRAUD

Figures rounded to closest whole number



ORDER PROCESSING RATES FOR MANUAL REVIEW VARY DRAMATICALLY

In larger companies each reviewer analyses over 100 orders per day; in others it can be as few as ten.

	MEAN
🏠	11
🏪	41
🏢	96
🏬	112
OVERALL	77

Chart 5:

AVERAGE NUMBER OF ORDERS REVIEWED (PER REVIEWER/PER DAY)

Base: 63. Figures rounded to closest whole number

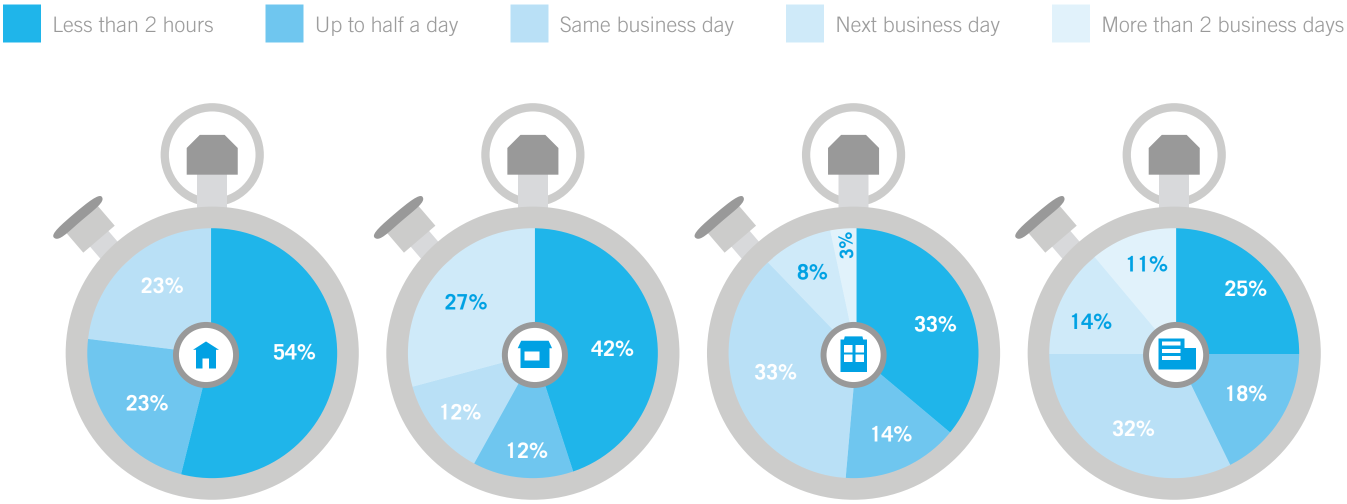
Not surprisingly, this number increases dramatically with the size of business. Larger merchants generally have more mature processes and have deployed additional tools to help streamline review. Or they have outsourced this operation altogether.

LARGE MERCHANTS CLEAR ORDERS IN 1 BUSINESS DAY; SMALL MERCHANTS IN UNDER 2 HOURS

Smaller businesses are more likely to address an order soon after it arrives, leading to a shorter review period.

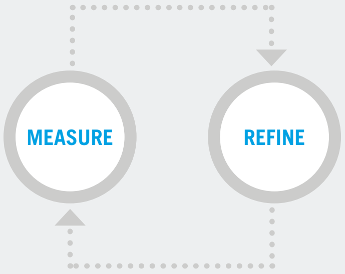
With much higher transaction volumes, larger organisations need an effective queue system to efficiently process priority orders and maintain customer satisfaction. A more systematic and organised approach to manual review is required, for example building in peak-time planning, priority shipping and gold customer status.

Chart 6:
TIME TAKEN TO REVIEW ORDERS
Excluding 'don't know' responses



TAKE ACTION

OPTIMISE YOUR REVIEW:



Review teams often comprise the biggest part of the fraud management budget, so monitoring and improving performance is critical. To optimise review, look to:

1. Balance effectiveness against efficiency; measuring key performance metrics both by reviewer and more broadly. Include:
   - Chargebacks
   - Review time
   - Number of transactions reviewed
2. Use a case management system to bring more structured review and gather KPIs. Measure and review results against overall fraud management KPIs for a specific period of time to determine trends and areas for improvement. CyberSource Decision Manager includes advanced case management as standard.
3. Ensure your fraud teams constantly share knowledge about the latest trends, and that they understand which information sources/validation databases work best in different markets.

A global presence, combined with cross-vertical expertise and access to more data, helps our review teams identify new fraud trends faster, providing customers with peace of mind.

Travis Barratt
Manager, CyberSource Screening Management

71%

of Manually Reviewed Orders are Accepted

54% of merchants surveyed ultimately accept over 90% of reviewed orders; manual review can prove hugely inefficient for many businesses.

As a rule of thumb, half of reviewed orders should be accepted; excessively high or low acceptance rates suggest that there are inefficiencies and that rules should be reviewed.

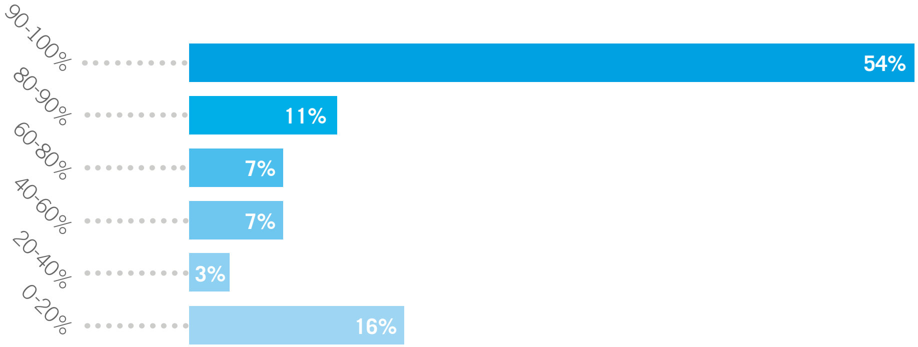


Chart 7:
% OF REVIEWED ORDERS ULTIMATELY ACCEPTED
Base: 91

TAKE ACTION

TURN REVIEW INTO RULES

At CyberSource, we pay close attention to the orders that our reviewers accept, looking for common characteristics including:

- Products ordered
- Geolocation elements (e.g. correlating BIN, shipping/billing address and IP location)
- Velocity characteristics
- Device configuration (e.g. whether Flash, JavaScript or cookies are enabled; browser language; device clock time zone)

We use this analysis to create rules, allowing those orders to be automatically accepted in the future. The result? A vastly improved customer journey.

4%

of Overall Orders are Rejected on Suspicion of Fraud

False positives contribute significantly to the total cost of fraud. Physical goods retailers reject a mean average of 6% of orders for fear of fraud.

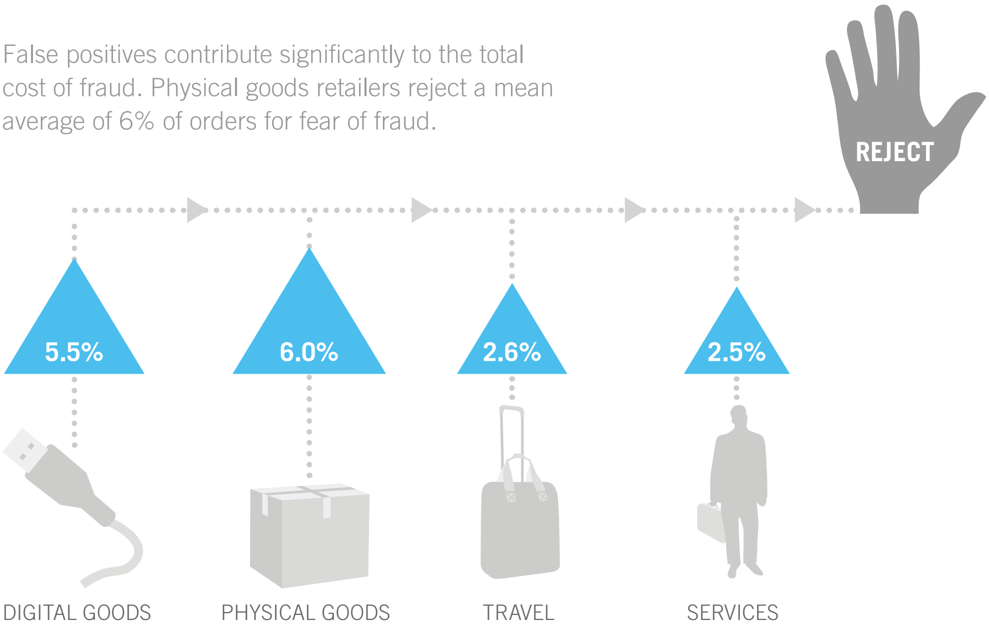
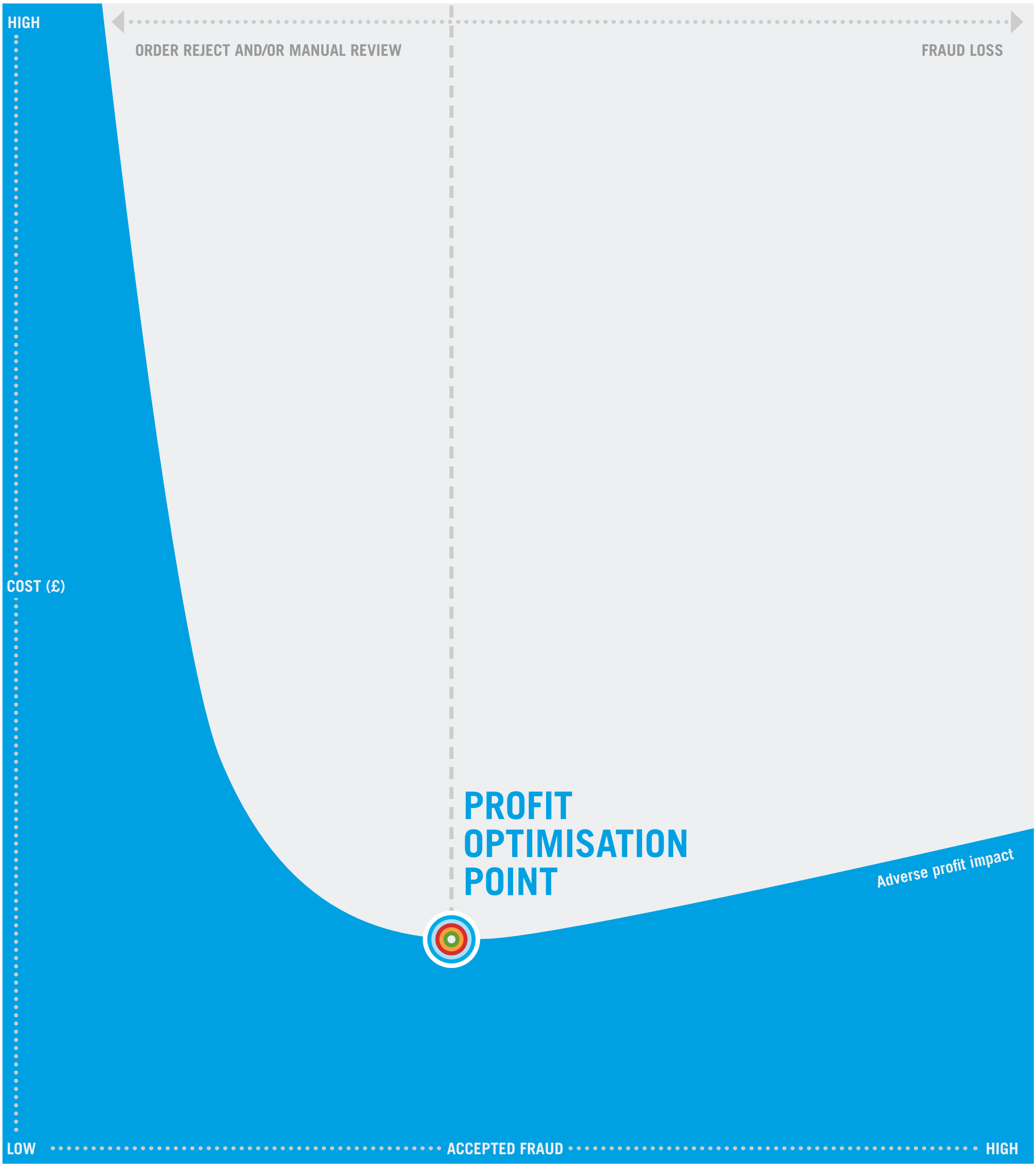


Chart 8:
AVERAGE % OF ORDERS REJECTED DUE TO SUSPICION OF FRAUD
Figures rounded to one decimal place

STRATEGIC FOCUS: OPTIMISE PROFITS

Calculate your profit optimisation point to find the balance between being too relaxed and too strict with fraud strategies. This will vary by business and depend on the type of goods sold, markets served and level of risk aversion.

Chart 9:
PROFIT OPTIMISATION POINT



Largest Merchants FIGHT 47% of Chargebacks

Whilst merchants re-present on average 29% of fraud chargebacks, 44% dispute less than one in ten. Overall, respondents win under a third of re-presented fraud chargebacks; 40% actually win less than 10%.

Scale and maturity can bring the more advanced processes required to tackle chargebacks effectively. Re-presenting transactions can have a dramatic impact on total fraud losses.

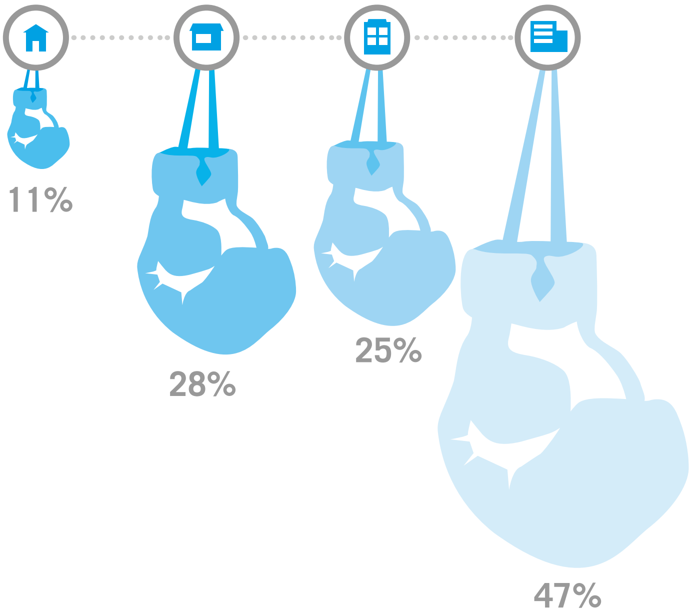


Chart 10:
% OF FRAUD CHARGEBACKS RE-PRESENTED
Base: 63. Figures rounded to closest whole number

SIZE OF BUSINESS
- Small
- Medium
- Large
- Very Large

On Average 0.5% of Accepted Orders Result in Fraud

The median fraud order rate is within expectations, and the variation between sectors not surprising.

For physical goods retailers, the ability to sell tangible goods quickly appeals to a greater number of fraudsters, whilst in the travel sector tickets are often stolen to order.

For the services industry, once it becomes apparent that the organisation has been defrauded the service will likely be halted – acting as a deterrent for fraudsters since the potential gains are limited.

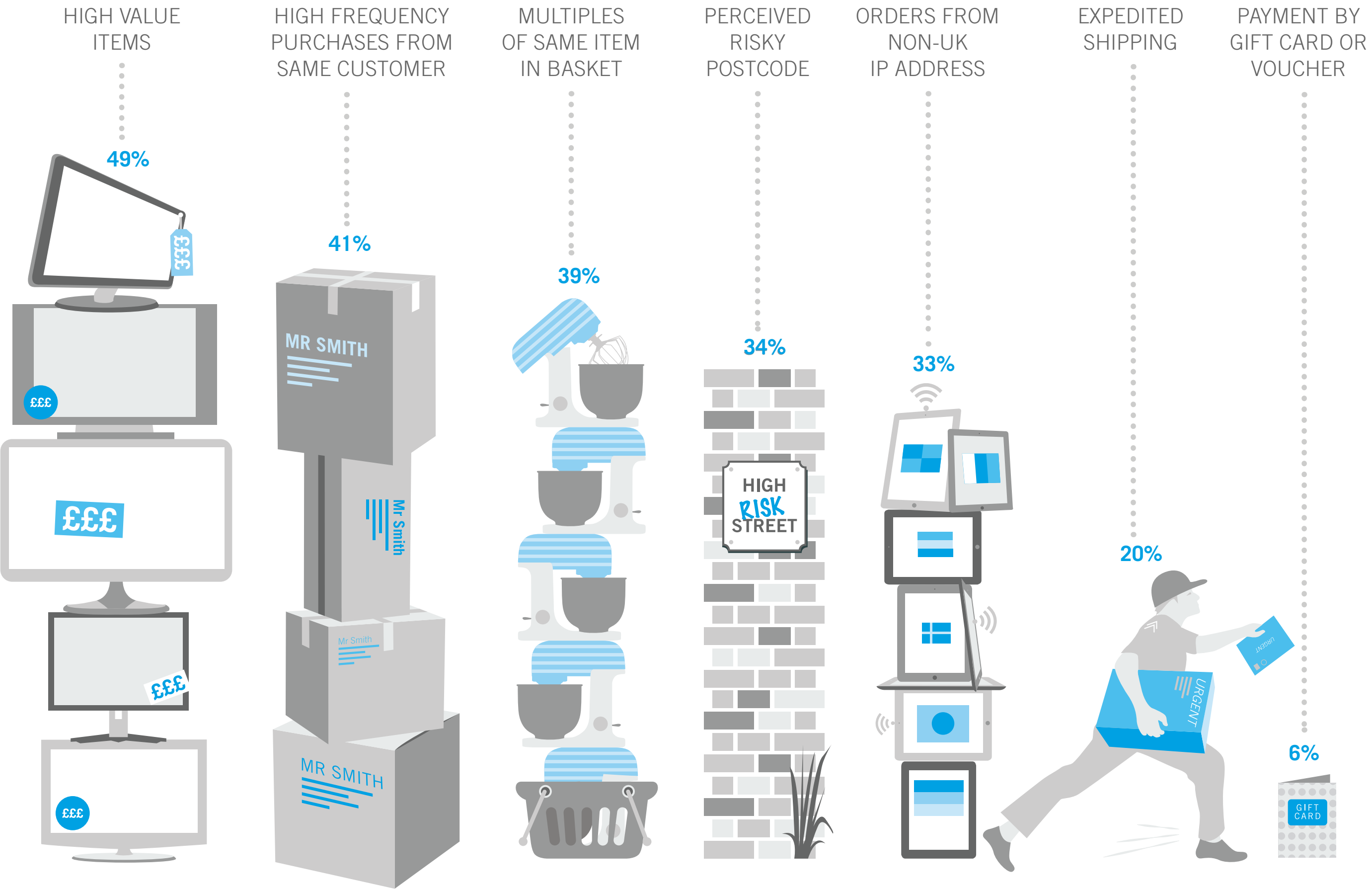
DIGITAL GOODS	0.75%
PHYSICAL GOODS	1%
TRAVEL	0.5%
SERVICES	0.1%

Chart 11:
AVERAGE % OF ORDERS LATER RESULTING IN FRAUD

ITEM VALUE IS THE BIGGEST INDICATOR OF FRAUDULENT BEHAVIOUR

The nature of the transaction can be a powerful indicator of fraud, flagging an order for greater scrutiny. Higher value items and high frequency of purchase lead the field in terms of suspicious behaviour.

Chart 12:
MOST COMMON INDICATORS OF HIGH RISK TRANSACTION



TAKE ACTION

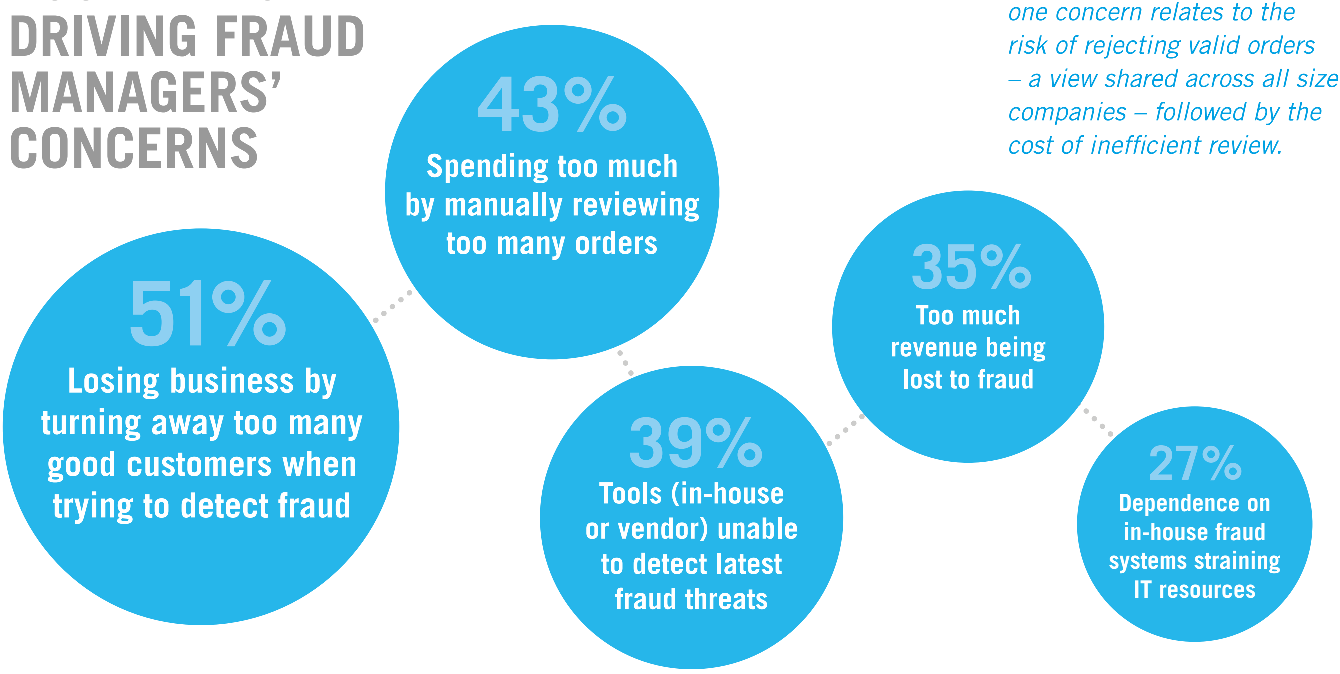
INVEST IN SMARTER RULES

Fraud attacks will change over time, often rapidly. To respond quickly you'll need to build and deploy new rules in real-time, and have the means to test the impact of these rules before they go live. Check that your fraud management system has this functionality.

Survey respondents cited that high value transactions are risky. Build smarter rules, e.g. only analyse higher value orders for customers that have placed less than three good orders with you. In doing so, you can leverage your own historical data and accelerate good orders.

CUSTOMER ACCEPTANCE DRIVING FRAUD MANAGERS' CONCERNS

Chart 13:
TOP eCOMMERCE FRAUD CHALLENGES



Revenue loss now sits outside the top three challenges for fraud managers. The number one concern relates to the risk of rejecting valid orders – a view shared across all sized companies – followed by the cost of inefficient review.

TAKE ACTION

Ensure business rules are optimised upfront to help reduce the review rate, and improve the customer experience.

CHARGEBACK VALUE MOST POPULAR MEASURE OF ANTI-FRAUD SUCCESS

Chart 14:
TOP FRAUD METRICS MEASURED AGAINST

1 CHARGEBACK VALUE **43%**

2 OVERALL ACCEPTANCE RATE **41%**

3 OVERALL REJECT RATE **40%**

4 CHARGEBACK VOLUME **37%**

5 REVIEW RATE **19%**

A range of benchmarks are used to define the success of anti-fraud efforts. The top measurements (chargeback value, acceptance rate and reject rate) highlight the need to deliver maximum revenue from genuine customers, at the lowest cost to the business.

Interestingly, review rate is by far the lowest ranked metric; yet above merchants highlighted concerns about the cost implications of reviewing too many orders.

TAKE ACTION

Merchants should increase the focus on review rate as a measure of their fraud management efficiency.

03 | OPENING THE RIGHT DOORS

63%

of merchants accept international orders

13%

of merchants to start processing transactions from outside the UK in next 12 months

24%

of merchants don't accept orders from outside the UK and have no plans to do so

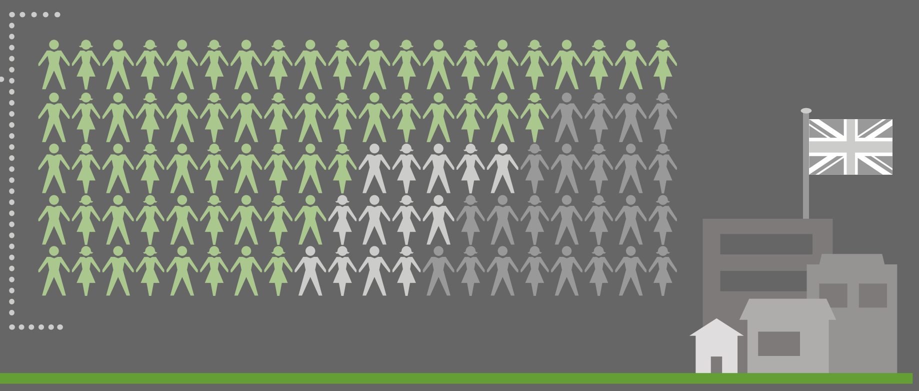


Chart 15:
% OF eCOMMERCE ORDERS FROM OUTSIDE UK

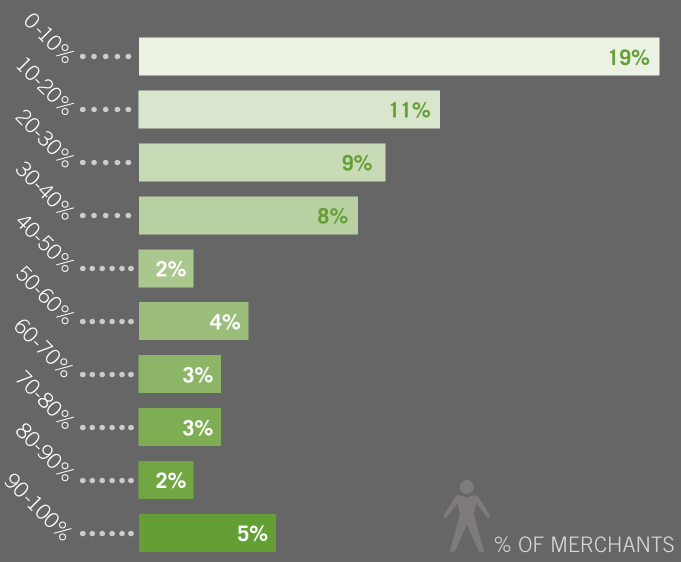
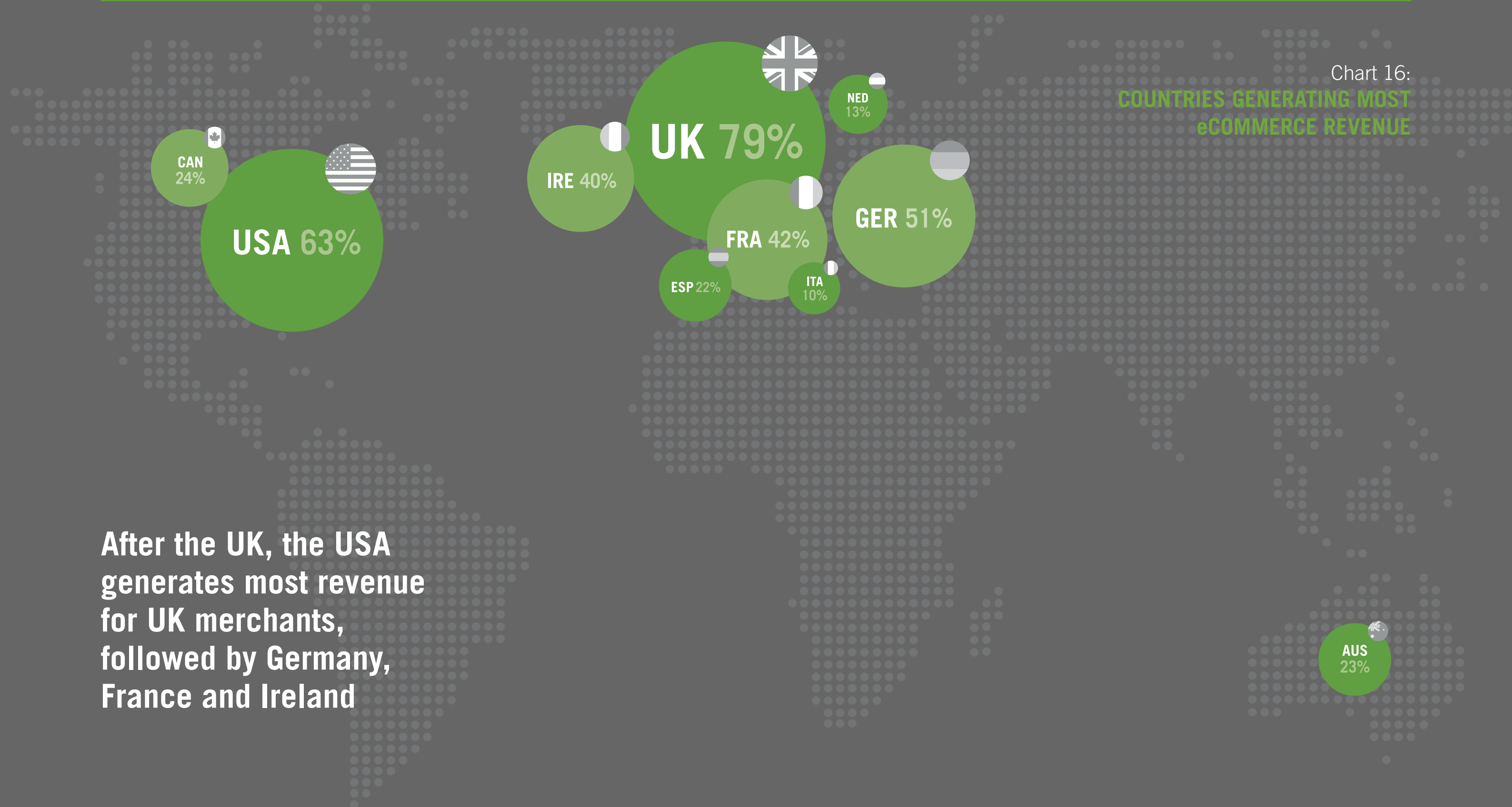


Chart 16:
COUNTRIES GENERATING MOST eCOMMERCE REVENUE



After the UK, the USA generates most revenue for UK merchants, followed by Germany, France and Ireland

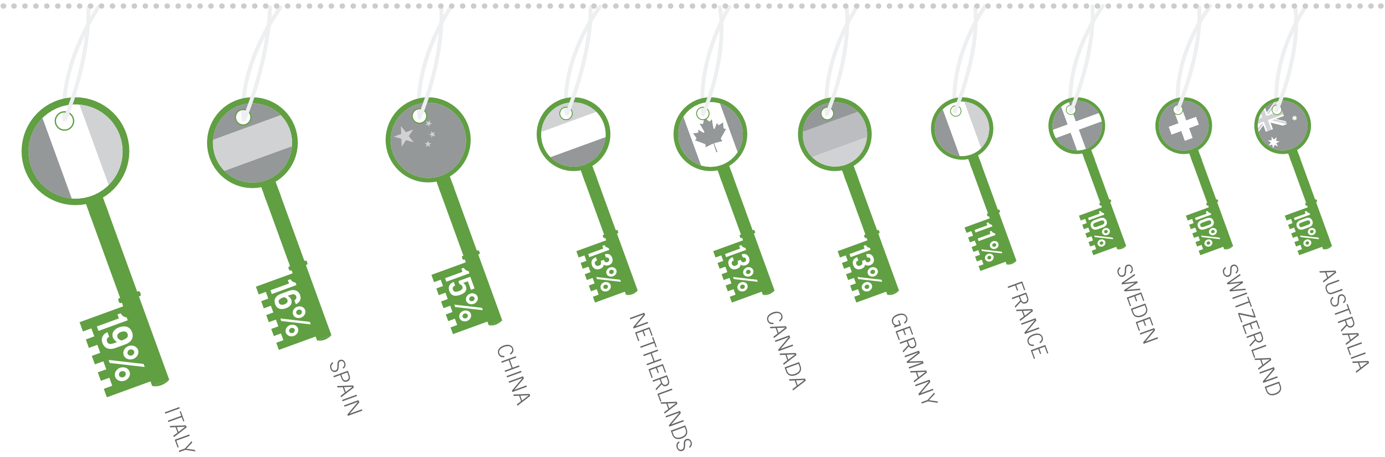
ITALY, SPAIN AND CHINA

Top of Target List

In spite of the economic situation in southern Europe, Italy and Spain are hot target territories for UK merchants in 2013.

There are clear opportunities in the BRIC countries if trust issues can be overcome, with A.T. Kearny's 2012 eCommerce Index identifying China, Brazil and Russia as the emerging markets that offer the greatest eCommerce potential for retailers looking to expand.

Chart 17:
TOP COUNTRIES PLANNED FOR MARKET ENTRY



SPOTLIGHT ON GLOBAL FRAUD

Offering worldwide coverage, our Managed Risk Analysts provide the regional insight you need to expand safely. Here's a snapshot:

BRAZIL: It's important to have controls in place around zip codes as fraud is regionalised. We recommend that merchants also capture the customer's CPF number (similar to the US Social Security Number) as part of the checkout process.

FRANCE: Fraud is also regionalised; however French Territories can present a challenge. For example, Guadeloupe has its own ISO Country Code, yet any credit cards issued here are typically assigned directly to France. This means that rules based on BIN mismatches need careful consideration.

CHINA: Domestic fraud is low, however due to the large export business cross border fraud can be high. Banks in China typically do not have processes in place for cardholders to report fraudulent transactions, so reclaiming funds can be very difficult.

INDIA: It's extremely common for consumers to share credit card numbers when buying online, especially from travel websites; thus rules need to be configured differently. 3D Secure is mandated for online purchases, therefore chargeback liability shifts can apply.

GETTING THE RIGHT BALANCE

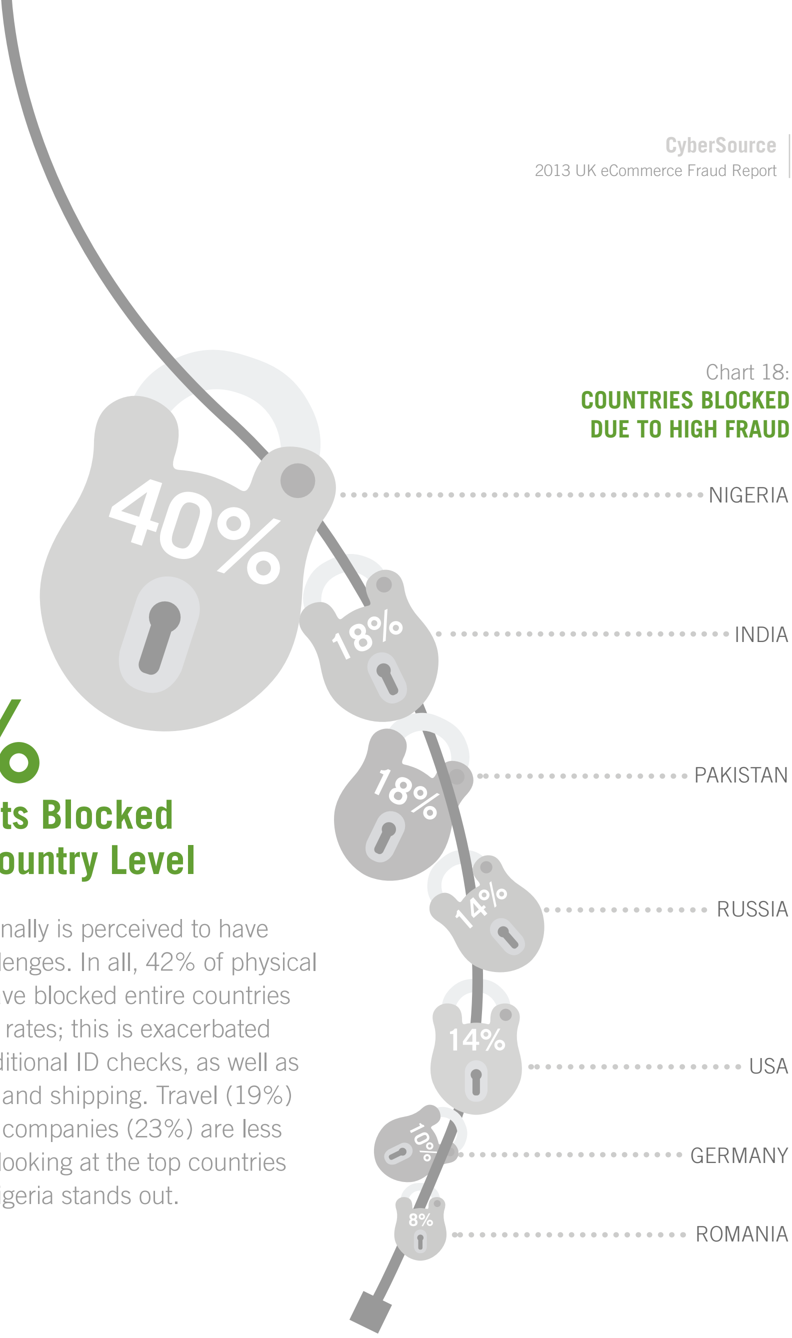
1. ARE YOU BLOCKING GOOD CUSTOMERS?

26%

of Merchants Blocked Orders at Country Level

Trading internationally is perceived to have a number of challenges. In all, 42% of physical goods retailers have blocked entire countries due to high fraud rates; this is exacerbated by the lack of additional ID checks, as well as the cost of goods and shipping. Travel (19%) and digital goods companies (23%) are less impacted. When looking at the top countries being blocked, Nigeria stands out.

Chart 18:
COUNTRIES BLOCKED DUE TO HIGH FRAUD



2. HOW DO YOU MANAGE ALTERNATIVE PAYMENTS?

65%

Accept Non-Card Payments

Alternative payment methods are increasingly part of the mainstream eCommerce purchase.

One in four merchants don't scan non-card payments for fraud. With 37% only scanning those non-card orders considered 'risky', screening processes are not as well configured for alternate payments.

We're seeing the ability to pay with one set of stored details across multiple retailers have growing appeal, particularly on mobile devices with their smaller screens and limited interfaces. This, alongside increased consumer understanding, will likely help drive acceptance.

TAKE ACTION

We can help you understand the risk profile for different payment types and employ the right fraud strategy. For example, with online bank transfers businesses are well-protected with little fraud liability, whereas direct debits can result in greater exposure; long windows are open within which consumers can initiate a chargeback.

04 | THE CHANGING FACE OF eCOMMERCE

CHALLENGE: NO CONSOLIDATED VIEW

The reality of eCommerce in 2013 is that it encapsulates many routes to market; today's consumers are truly connected.

Of the web merchants surveyed:

41% operate a mobile commerce website or app

65% also have a telephone or mail order channel

54% have physical stores

9% accept kiosk payments

78% screen mobile channel using existing eCommerce fraud tools

Each channel can present a different challenge, with myriad fraudster tactics. Yet 18% of merchants don't currently screen fraud by order channel at all, climbing to 52% amongst smaller businesses.

Chart 19:
CHANNELS TRACKED FOR FRAUD

Telephone/Mail order channel	41%
Physical/Face to face	29%
Mobile	27%
Kiosk	6%
Do not track by channel	18%

Lack of channel-specific screening could hide fraudster tactics or fraud rates. With mobile commerce growing, it's vital that merchants understand the impact of fraud across multiple touchpoints.

Organisations should ensure that their tools are suitably configured to take account of the different factors and attributes of each channel; for example the reduced chance of a successful geographic IP lookup on a mobile device, or the increased likelihood that orders from such devices may be placed at unusual times of day.

TAKE ACTION

CONSOLIDATE WHERE IT MATTERS

We recommend that merchants screen all transactions, across web, mobile, call centre channels, on one platform. This single view of the customer will help improve their experience, particularly if you are storing card details and can accommodate one click checkout. Focus attention where it matters most: optimising the entire journey, and not just the touchpoint.

- Ensure that any platform selected has the flexibility to screen orders from different channels using different rule sets;
- The power comes through tracking attempted transactions from multiple sources using cross-channel velocity checks. For example, if an order is being placed via your call centre, it's useful to know if that customer has just been rejected on your web store for providing an incorrect 3D Secure password. This would be typical behaviour for a fraudster using a stolen card.

MOBILE FRAUD RATES VARY ACROSS SECTORS

Today there is only a small base of merchants who break out fraud rates by channel; of those that do, mobile rates appear to be marginally higher for digital goods and marginally lower for travel.

Across all sectors, there is a relatively even split when comparing fraud rates between mobile commerce websites/apps and webstores. 42% of respondents report the mobile rate is no different to their webstore; 22% suggest it is higher; 36% lower. Until there is more data it is too early to understand the true picture.

The mobile channel presents a tremendous opportunity for businesses, but also poses some risk, as typical validation tools available through the web are not as effective for mobile. At the same time, mobile phones provide rich data to companies to validate the consumer, especially through a mobile app.

TAKE ACTION

ACCEPT GENUINE MOBILE CUSTOMERS, FASTER

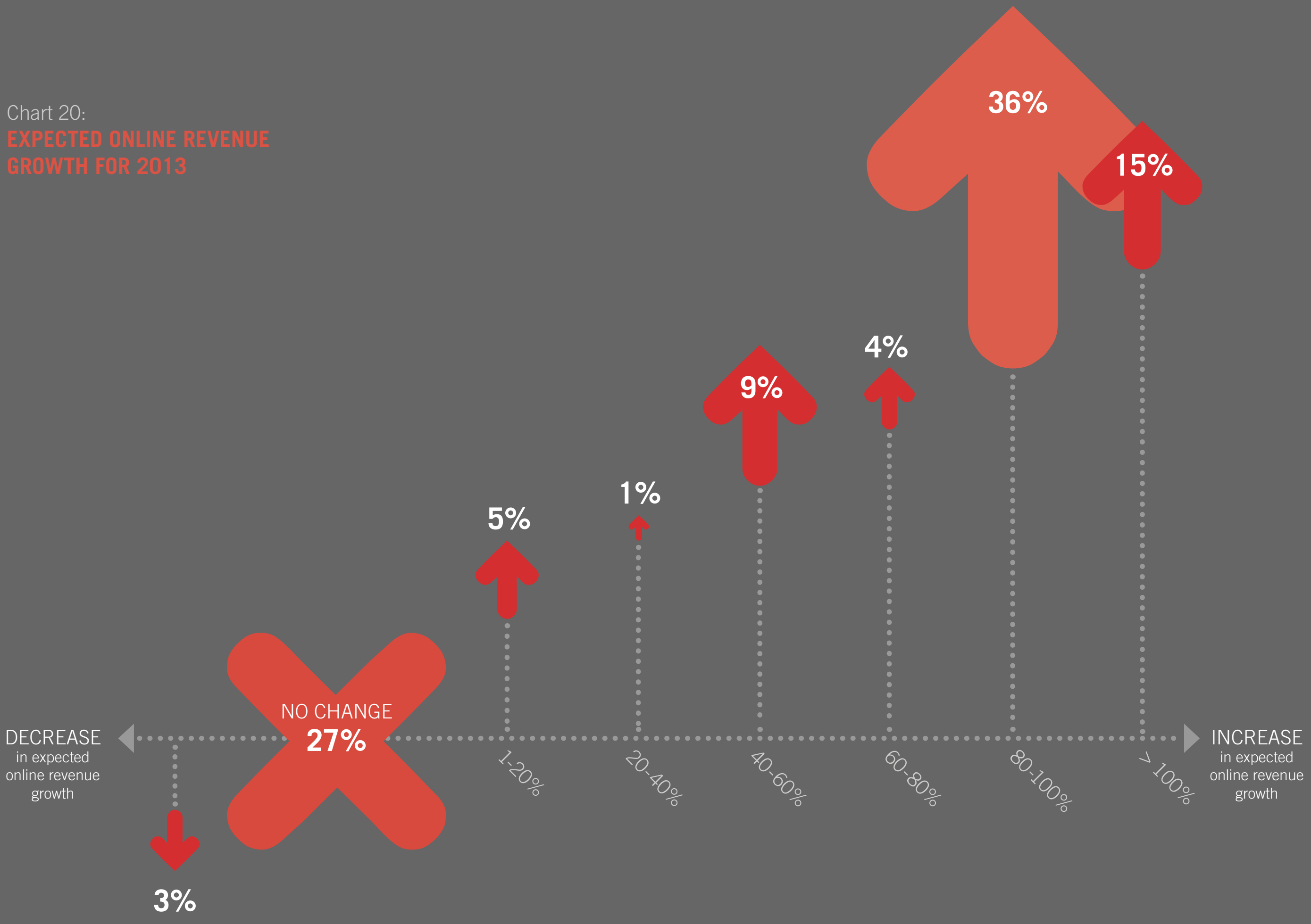
1. Closely monitor and track behaviour for transactions that come from mobile devices and cross-check against other historical data. If a customer uses an app to purchase, you can potentially obtain additional information to use in your screening rules.
2. Utilise and create rules around device fingerprinting, proxy piercing and VPN detection. For example, with iOS, Android, and Windows 8 devices, fraudsters can bypass the pre-installed browser and use one that they've downloaded instead, enabling them to create proxy sites that mask their actual location. Similarly, free VPN solutions enable fraudsters to select an originating IP address. As VPN solutions are often customised, traditional detection routines do not work as efficiently.
3. Factor the presence of malware and other unauthorised software running on the mobile device into your fraud screening strategies. Mobile malware, like PC malware, can steal account credentials, take over sessions, perform injection attacks and corrupt browsers and apps engaged in logins and transactions.
4. If you have a dedicated mobile app, promote its use to your customers. Apps can provide much better separation on the device (sandboxing) and stronger OS-level protection.

Aarij Khan
Senior Director Product Marketing, ThreatMetrix

eCOMMERCE CONTINUES TO OFFER THE GROWTH OPPORTUNITY FOR 2013

Confidence in UK eCommerce is fairly high for many organisations, despite the sluggish economy. In all, 27% of merchants believe there will be no change to their eCommerce revenues. For those expecting growth, an average increase of 26% is forecasted. Whilst this applies across all scales and sectors of the market, small and medium businesses estimate the highest growth rates.

Chart 20:
EXPECTED ONLINE REVENUE GROWTH FOR 2013



85%

of Merchants Expect Fraud Revenue Losses to Remain Static or Grow in 2013

Unfortunately confidence does not extend to the ability to cut fraud, with most expecting fraud losses to sustain (53%) or increase (32%) as a proportion of eCommerce revenue. This is certainly a concerning trend, with similar results reported in the previous survey.

IMPROVING AUTOMATED FRAUD DETECTION

Top Priority for 2013

Chart 21:

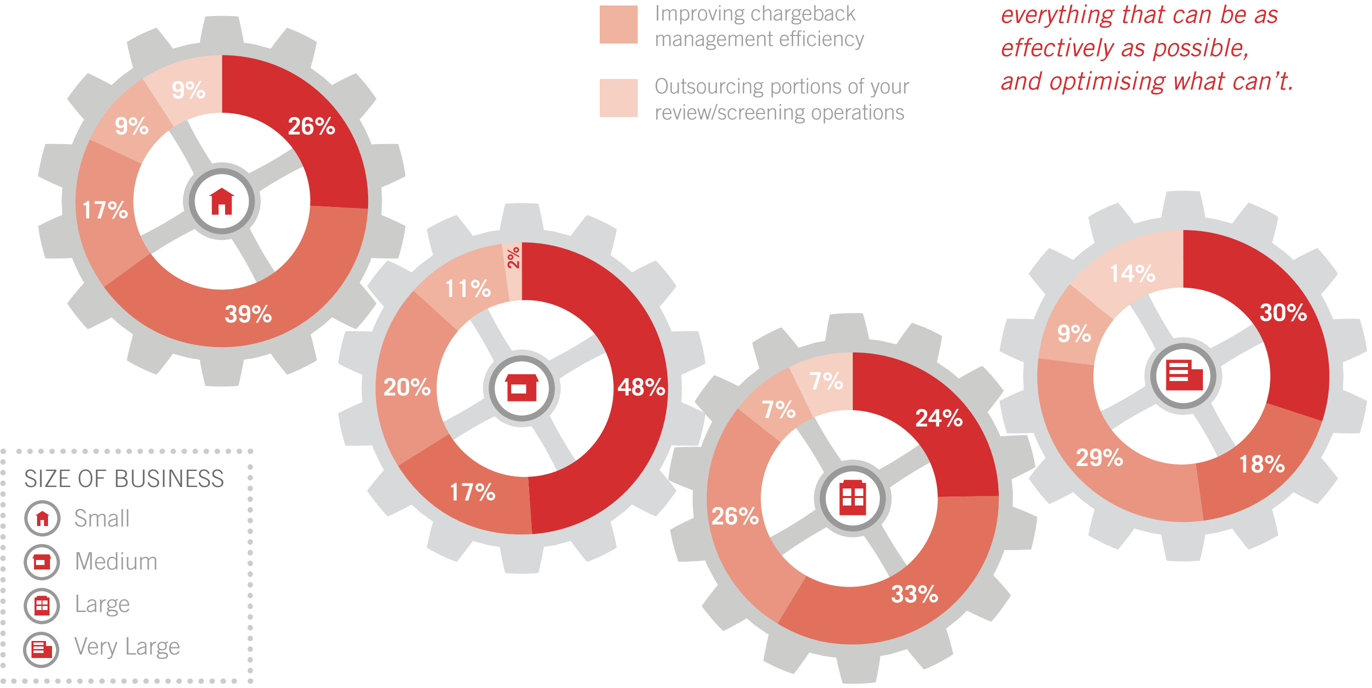
TOP BUSINESS PRIORITIES FOR 2013

Excluding ‘don’t know’ responses

- 🟥 Improved automated detection and sorting accuracy
- 🟥 Streamlining the tasks/workflow occurring during the manual review process
- 🟥 Improving process analytics
- 🟥 Improving chargeback management efficiency
- 🟥 Outsourcing portions of your review/screening operations

In focusing on automation, merchants can help ensure that the highest possible volumes of genuine customers are accelerated through; newer, cleaner types of fraud are identified; and the burden of manual review is cut.

Priorities are tied to automating everything that can be as effectively as possible, and optimising what can’t.



TAKE ACTION

IMPROVE AUTOMATION: CREATE LAYERS

The goal of any fraud management strategy should be to accurately identify and accept good orders, while keeping fraudsters out. We advocate that you use ‘layers’ of detectors, built using specific techniques:

1. **CORNERING:** 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);
2. **DIMENSIONALITY:** Once you have the key piece of information, add ‘dimensions’ of related data that you have about the order (e.g. device fingerprint, account number, email), then build rules using the combined datasets. For example, create rules with shipping address + velocity intervals AND shipping address + account number(s). This makes it more difficult to perpetrate fraud systematically;
3. **SPECIFICITY:** Take advantage of any specific items of data that you’ve seen used in historic fraudulent transactions, such as devices or email addresses, and ensure they can’t be used again through robust negative listing. This forces the fraudster to constantly seek new identities, devices or payment data to try and break through your defences. Although simple to execute, it is typically seen as the final layer of your fraud strategy.

Say Manual Review Staff Won't Increase in Next 12 Months

The biggest organisations are planning the smallest increases in manual review staff, with 10% looking to cut the size of their review teams.

Today, it is much more common to outsource this function; over a quarter of larger merchants are planning just this. Those businesses not looking to outsource cite quality of service as a concern – we do see differing standards across vendors.

TAKE ACTION

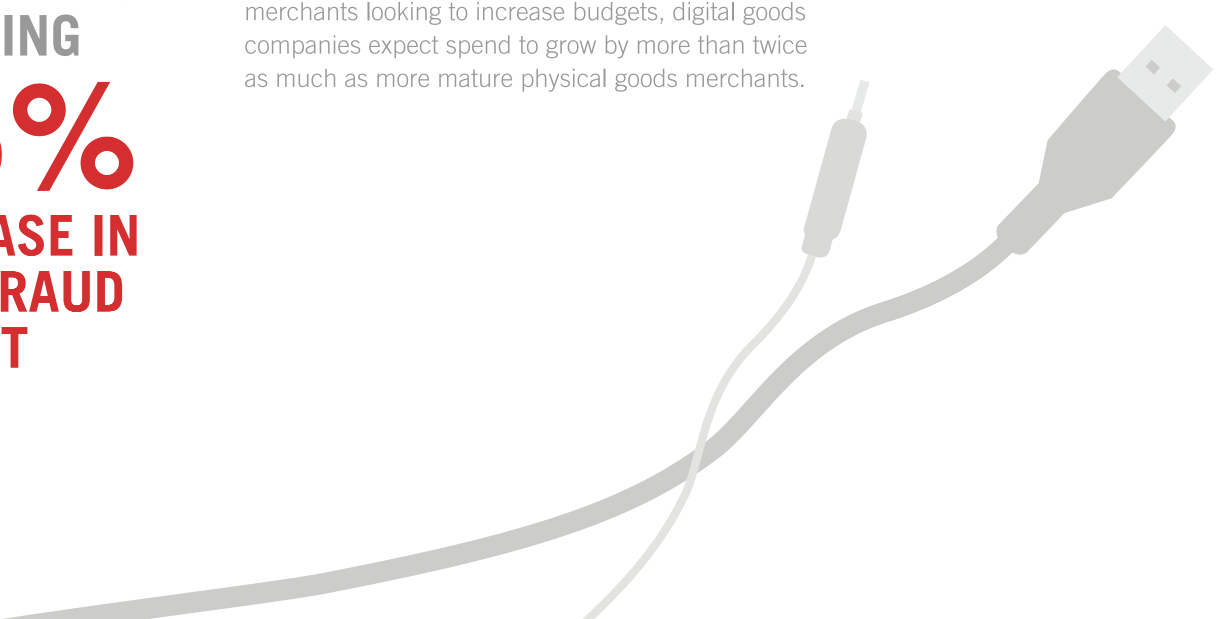
PRIORITISE QUALITY

Use the following checklist when evaluating whether to outsource your manual review function:

1. Ensure the provider has the skills and technology required to effectively review orders (which checks, in which order, how to weight them, how to keep an audit trail of actions on each order);
2. Flexibility is key; confirm that they can adapt to meet your changing needs (including new products and markets, as well as promotions);
3. If you would like the provider to interact with your customers, ensure this is transparent (e.g. email domains, dedicated phone numbers, call scripts);
4. Make sure they sign up to your company values and code of ethics;
5. Agree appropriate SLAs well in advance (e.g. fraud rate, review rate, response time), and ensure that penalties are in place if the SLA is not met;
6. Confirm quality assurance processes; our team follows set procedures when reviewing orders and results are constantly evaluated.

DIGITAL GOODS MERCHANTS PLANNING 36% INCREASE IN ANTI-FRAUD BUDGET

Most businesses (69%) are not looking to increase their fraud management budgets for the year ahead, with only the largest investing at scale. Of those merchants looking to increase budgets, digital goods companies expect spend to grow by more than twice as much as more mature physical goods merchants.



06 | IN CONCLUSION

The survey results have revealed a clear opportunity for merchants. This centres on the need to address the business lost by turning away too many good customers, combined with inefficient review practices.

It is clear from the report that, in itself, the fraud rate is not the most important factor. What is crucial is the impact this rate has on profit. Historically we've seen a focus on minimising the number of fraudulent orders, sometimes to the detriment of business elsewhere. And whilst continued investment is required to ensure that 'cleaner' fraud can be caught sooner, if adopted in isolation this investment can deliver diminishing returns.

Consider the order rejection rate: merchants reject over 4% of orders on suspicion of fraud. This climbs to almost 6% for physical goods retailers. Thus, it's no surprise that the number one concern for respondents of all sizes is the rejection of good orders, and the impact that this has on the wider organisation.

In 2013 merchants should refocus on driving acceptance; identifying good customers sooner, building on positive data and lists, removing friction from the checkout process. In doing so, businesses can better control short and longer term profits and improve the overall experience.

Do better with less

With fraud management budgets static for the majority in 2013, it's vital to maximise returns, particularly as new markets and sales channels are explored. There is much room for improvement, with just over half of respondents ultimately accepting over 90% of reviewed orders; a trend that has not changed substantially during the last few years.

Improving automated front line screening can dramatically reduce the need for manual review, allowing budgets to be reallocated elsewhere. And a focus on rule optimisation helps ensure that genuine customers are rapidly identified upfront and sped through the checkout process, irrespective of touchpoint. The end game? More eCommerce customers. Accepted faster; safely; everywhere.

FRAUD MANAGEMENT, REFOCUSED

We help businesses to identify genuine customers sooner, with a range of flexible and powerful options that automate and optimise fraud management. Spanning training, expert consultation and monitoring of fraud strategies, as well as outsourced review operations, we address your specific requirements.

DECISION MANAGER AND MANAGED RISK SERVICES

Decision Manager, our hosted fraud management system, is the foundation; providing access to data generated from global fraud detectors, multi-merchant and cross-industry correlations, and much more. The system features a highly flexible rules engine with powerful statistical risk models and customisable case management, all backed by extensive analytics. Built for your needs, Decision Manager can be operated by you, us or together.

CHARGEBACK MANAGEMENT SERVICE

CyberSource chargeback experts perform detailed analysis of your chargebacks and provide insights into your fraud operations to prevent future occurrences. We manage the entire recovery process – receipt and review, interaction with banks, and re-presentment documentation – to ensure that you maximise profitability with the least impact to your operations.

To find out about our wider fraud, global payment and security solutions, please call your local office. You'll also find self-paced webinars, white papers and demos at:
cybersource.co.uk

FOR MORE INFORMATION

UK/EUROPE
Call +44 (0) 118 990 7300 or email **uk@cybersource.com**

SUB-SAHARAN AFRICA
Call +27 11 547 8463

MIDDLE EAST AND NORTH AFRICA
Call +9714 457 7200

RUSSIA
Call +7 (495) 787 45 24

For a complete list of worldwide offices go to cybersource.com/locations

ABOUT CYBERSOURCE

CyberSource, a wholly owned subsidiary of Visa Inc., is a payment management company. Over 400,000 businesses worldwide use CyberSource and Authorize.Net brand solutions to process online payments, streamline fraud management, and simplify payment security. The company is headquartered in San Francisco and maintains offices throughout the world, with regional offices in Singapore (Asia Pacific), Tokyo (Japan), Miami (Latin America and Caribbean), and Reading, UK (Europe/Middle East/Africa). CyberSource operates in Europe under agreement with Visa Europe.

For more information, please visit cybersource.co.uk

CyberSource has chosen the most environmentally responsible method of printing for this report. Printed with minimum impact on the environment: zero waste to landfill, 100% recycled FSC paper, 100% vegetable oil-based inks, 100% renewable power, 100% carbon neutral, 100% alcohol free and 100% waterless.

Designed by pinkgreencreative.co.uk

TOMORROW IS NOW

At CyberSource, we are dedicated to helping our customers embrace the speed of eCommerce change. A sophisticated payment and fraud management platform helps merchants innovate faster, so that they can accept more customers, from across more markets, via more devices. Safely.

A single connection makes light work of integration; whilst our global footprint means that we can scale as merchants expand, driving out complexity and enabling growth.

And with over 19 years' experience, we're able to gather intelligence from over 400,000 customers based round the world, continually evolving our enterprise-calibre solutions.

CyberSource®
the power of payment

cybersource.co.uk